Computer Access Technology Corporation

2403 Walsh Avenue, Santa Clara, CA 95051-1302 Tel: +1/408.727.6600 Fax: +1/408.727.6622

CATC Merlin Mobile™

Bluetooth™ Protocol Analyzer

User's Manual

Document Disclaimer

The information contained in this document has been carefully checked and is believed to be reliable. However, no responsibility can be assumed for inaccuracies that may not have been detected.

CATC reserves the right to revise the information presented in this document without notice or penalty.

Trademarks and Servicemarks

CATC, Merlin, Merlin's Wand, Merlin Mobile, BTTracer, BTTrainer, Advisor, Chief, FireInspector, Inspector, Detective, Traffic Generator, BusEngine, USB4DOS, UPT, HPT, UHT, IBTracer, and *SATracer* are trademarks of Computer Access Technology Corporation.

Microsoft, Windows NT, *Windows 2000*, *Windows* 98*SE*, *Windows Me*, and *Windows XP* are registered trademarks of Microsoft Inc.

All other trademarks are property of their respective companies.

Copyright

Copyright © 2003, Computer Access Technology Corporation (CATC); All Rights Reserved.

Portions of this product are supplied courtesy of Richard Herveille. Copyright (c) 2002, 2003 Richard Herveille, rherveille@opencores.org. All rights reserved.

This document may be printed and reproduced without additional permission, but all copies should contain this copyright notice.

FCC Conference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device and an intentional radiator, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense. The end user of this product should be aware that any changes or modifications made to this equipment

without the approval of CATC could result in the product not meeting the Class A limits, in which case the FCC could void the user's authority to operate the equipment.

Important Notice: To comply with FCC RF exposure requirements (sections 1.1307 and 1.310 of the Rules) only the antenna supplied by CATC must be used for this device. The antenna must be located at least 20 cm away from all persons.

FCC Testing applies to FCC ID: KH7BT004APA-X.

EU Conference Statement

This equipment complies with the R&TT Directive 1999/5/EC. It has been tested and found to comply with EN55022:1994/A1:1995/A2:1997 Class A, EN61000-4-2:1995, EN61000-4-3:1995, EN61000-4-4:1995, EN61000-4-5:1995, EN61000-4-6:1995, EN61000-4-11:1994, EN61010-1:1993, and ESTI EN 300 328-1 V1.2.2 (2000-07).

TABLE OF CONTENTS

Chapter 1 Overview 1
Bluetooth Specification 2
Merlin Mobile Analyzer System Components 2
Merlin Mobile Specifications 2
System Requirements 3
Using Merlin Mobile with Merlin's Wand 3
Merlin Mobile Automation 3
HCI Trace 4
Features of Merlin Mobile 4

Chapter 2 Getting Started 7
Installing Merlin Mobile 7
Software Installation 7
Hardware Installation 7
Starting and Stopping Merlin Mobile 8
Starting the Application 8
Exiting the Application 8
Starting the Analyzer Unit 8
Shutting Down the Analyzer Unit 8
Displaying Help 9
Updating the BusEngine and Firmware 9
Updating the Driver 9
Updating the Driver on Windows 2000 9
Updating the Driver on Windows 98 SE 10
Updating the Driver on Windows Me 11
Updating the Driver on Windows XP 12
License Keys 12
Update License 12
License Information 13
Installing the HCI Probe 13
HCI Probe configurations 14
2-port RS232 to USB converter 16
Your First Bluetooth Recording 17
Inquiry Recording 20

Chapter 3 Software Overview 23
The Main Display Windows 23
Toolbar 26
Status Bar 28
Recording Progress 28
Status Bar Position Definitions: 28
Recording Status 29
Analyzer Status 30
Search Status 31
Zoom In 31

Zoom Out 31
Tool Tips 31
Merlin Analyzer Keyboard Shortcuts 31

Chapter 4 Recording Wizard 33

Starting Recording Wizard 33
Recording a Traffic on a New Piconet 34
Recording an Existing Piconet 44
Recording in Test Mode 54
Recording in Reduced Hopping Mode 54
Recording in Single Frequency Mode 59

Chapter 5 Recording Options 63

Recording Modes 63
Piconet recording 63
Inquiry recording 63
IUT:HCI mode 64
Opening the Recording Options Dialog Box 64
Recording Options - General 65
Recording type 65
Options 66
Buffer Size 66
Trigger Position 67
Recording Options - Piconet 67
Hop Sequence 68
Sync Method 69
Additional Settings 73
Debug 75
Recording Options - Inquiry 75
Recording Options - HCI 76
HCI Window Layout 77
Recording HCI Traffic 79
Recording Options - Events 80
Payload Length Error 87
Recording Options - Actions 87
Action Buttons - Their Functions 88
Blue Dot Menus 90
Saving Recording Options 95
Recording Bluetooth Traffic 95

Chapter 6 Display Options 97

General Display Options 98
Setting Color, Formatting, and Hiding Options 99
Setting Color Display Options 99
Changing Field Formats 100
Hiding Display Options 101
Level Hiding Options 101

Level Hiding Parameters. 102
Saving Display Options 103

Chapter 7 Reading a CATC Trace 105

Trace View Features 105
Interpreting the Displayed Information 105
Tooltips 106
Set Marker 106
Edit or Clear Marker 107
Expanded and Collapsed Data Formats 108
Hide Frequency Hops. 110
Hide Nulls and Polls. 110
Hide ID Packets 111
Hide Voice (SCO) Packets. 111
Menus in Clicked Fields. 111
Hide Unassociated Traffic 111

Chapter 8 Decoding Protocols. 113

Introduction 113
LMP and L2CAP Messages. 113
Decoding and Viewing Protocol Data 114
Decoding Via the Decoding Toolbar 114
Decoding Via the Display Options Dialog Box 115
Tooltips 116
Viewing Packets in LMP and L2CAP Messages. 116
Types of LMP and L2CAP Messages 116
Viewing L2CAP Channel Connections 117
Viewing Protocol Messages and Transactions. 118
Viewing L2CAP Messages in Protocol Messages 119
How to Decode 119
Expanding Protocol Messages 119
Changing Protocol Assignments 120
Using the Decoding Assignments Dialog Box 120
Removing User-Assigned Protocol Assignments. 121
Manually Assigning Protocols 122
Other Assignments: OBEX Client/Server Status 122
Changing an OBEX Client or Server Status. 123
Decoding BNEP 123
Decoding HID. 123
Other Decoding Options 124

Chapter 9 Other Features 125

Search. 125
Go to Trigger. 125
Go to Packet/Message/Protocol 125
Go to Marker. 126
Go to 127

Error 130
Soft Bit Error 130
Loss of Sync 130
Find 130
Event Groups 132
Union, Intersection, and Exclusion 136
Using Find 136
Find Next 138
Device List 139
Edit Comment 140
Exporting Data 140
File Information 141
Error Summary 142
Timing Calculations 142
Bus Utilization 143
Traffic Summary 147
Encryption 147
Configuring Merlin Mobile for Encryption 148

Chapter 10 How to Contact CATC. 151

Chapter 11 Warranty and License 151

Index 153

1. Overview

The CATC™ Merlin Mobile™ Bluetooth™ Protocol Analyzer blends powerful piconet traffic recording and analysis abilities with compact, easily transportable PC Card technology. Merlin Mobile is a development and test tool for products using the Bluetooth wireless technology. Merlin Mobile non-intrusively monitors piconet traffic and records and displays captured Bluetooth data.

Like its predecessor, the CATC Merlin™ Bluetooth Protocol Analyzer, Merlin Mobile uses CATC's BusEngine™ technology, which incorporates a real-time recording engine with programmable data, state, and error detection, and event triggering, filtering, counting, and sequencing. This enables users to optimize recording memory usage to capture the data that is most important.

The Merlin Mobile system consists of the analyzer hardware unit and the analyzer software. The Merlin Mobile analyzer unit monitors and captures baseband packets on a piconet in a non-intrusive manner. The packets can then be viewed and decoded with the Merlin Mobile software. The software displays the piconet data in CATC Trace™ format and is capable of decoding and organizing the data for these Bluetooth protocol levels: Baseband, LMP, L2CAP, SDP, TCS, RFCOMM, OBEX, AT, HDLC, PPP, BNEP, HID, AVCTP, AVDTP, IP, TCP, and UDP. In addition, users can use the CATC Scripting Language (CSL) to create custom decoders for specific development purposes.

The Merlin Mobile analyzer unit is configured and controlled by the analyzer software. It can be used with portable computers for field service and maintenance, as well as with desktop units in a development environment. Furthermore, Merlin Mobile Automation™ and compatibility with the CATC Merlin's Wand™ Bluetooth Test Generator provide the capability for creating a fully-automated testing environment.

The Merlin Mobile analyzer includes provisions for on-the-fly detection of, and triggering on, numerous events. Such events include specific packet headers, payload headers, data patterns, and many abnormal (error) traffic conditions. Merlin Mobile continuously records the piconet data in a wrap-around fashion until it is manually stopped or until the trigger event is detected. Upon detection of a triggering event, the analyzer continues, as necessary, to record data until the recording buffer is filled.

The Merlin Mobile application may be used with or without the analyzer box. When used without the analyzer box, it functions as a CATC Trace™ viewer. As a Trace viewer, it can be used to view, analyze and print CATC Trace files.

1.1 Bluetooth Specification

Please refer to the Bluetooth Specification, version 1.1, for details on the Bluetooth wireless technology protocol. The Bluetooth Specification is available from the Bluetooth SIG at its web site: http://www.bluetooth.org.

1.2 Merlin Mobile Analyzer System Components

The Merlin Mobile analyzer package includes the following items:

- One Merlin Mobile analyzer unit
- Merlin Mobile software program installation CD
- Product documentation including on-line Help

1.3 Merlin Mobile Specifications

Package

Dimensions:	5.3 x 2.1 x 0.4 inches (135 x 54 x 5 millimeters)
Weight:	2 ounces (57 grams)

Hardware Interfaces

Connectors:	Standard 16-bit Type II PC Card
Antenna:	2.4 gigahertz external (ISM band)

Power Consumption

Idle:	300 milliamps (typical)
Active:	350 milliamps (typical)

Environmental Conditions

Operating Range:	0 to 55 °C (32 to 131 °F)
Storage Range:	-20 to 80 °C (-4 to 176 °F)
Humidity:	10 to 90%, non-condensing

Recording Memory Size

32 MB DRAM for traffic data capture
32 MB DRAM for timing, state & other data

Certification

Bluetooth version 1.1 qualified

Class 2 designation with +4dBm transmit power and <-70 receiver sensitivity

FCC and CE compliant

1.4 System Requirements

The following is the recommended configuration for the host machine that runs the Merlin Mobile Analyzer application and is connected to the Merlin Mobile Analyzer box.

- **Operating system:** Microsoft® Windows® 98 SE, Windows 2000, Windows ME, or Windows XP operating system.
- **Required setup:** Microsoft Internet Explorer 4 or later must be installed.
- See readme.html for the latest system requirements.

1.5 Using Merlin Mobile with Merlin's Wand

Merlin Mobile can be used in conjunction with the CATC Merlin's Wand™ Bluetooth Test Generator, which provides the ability to issue specific protocol commands and test sequences on a piconet. Using Merlin Mobile and Merlin's Wand together allows for real-time capturing of test sequence results as is required by the Bluetooth SIG to provide evidence of product compliance to the specification.

Merlin's Wand has built-in functionality for controlling Merlin Mobile. Through Merlin's Wand, a Bluetooth recording session can be set up on Merlin Mobile, even if the Merlin Mobile application runs on a remote computer.

For more information about using Merlin Mobile with Merlin's Wand, please consult the Merlin's Wand documentation or contact CATC.

1.6 Merlin Mobile Automation

The Merlin Mobile software includes an Application Program Interface (API) for developing testing programs and scripts in C++ and Visual Basic. The API reproduces most of the commands embodied in the Merlin Mobile trace viewer software. This API allows users to automate procedures that otherwise have to be run manually via the trace viewer software. The Automation API can be run locally on the PC attached to Merlin Mobile or remotely over a network connection.

For further details, refer to the *Automation API for CATC Bluetooth Analyzers* reference manual included in the installation CD-ROM. You can also download the document from the CATC website.

1.7 HCI Trace

In addition to the ability to record Bluetooth traffic off-the-air, using the analyzer's hardware and radio module, the Merlin can record serial Bluetooth HCI traffic from Bluetooth devices, or 'IUT's (Implementations Under Test).

While the off-the-air traffic is captured by the analyzers hardware, the HCI Traffic from the IUTs is captured by the analyzer application using an HCI probe (provided by CATC) that is connected directly to the IUT hardware. In a typical setup, the HCI commands and data to transmit are passed from the Bluetooth application to the Bluetooth baseband (Host to Controller), while events and data that was received are passed from the Bluetooth baseband to the Bluetooth application (Controller to Host).

To capture the data, the HCI Probe should be connected to the respective 'Host to Controller' and 'Controller to Host' lines. When the recording of the IUT's HCI is enabled and the application starts a recording, the serial data is captured as incoming serial data. For this, up to two COM ports should be configured for each IUT.

1.8 Features of Merlin Mobile

- Sophisticated software analyzes all piconet traffic
  - Identifies & highlights abnormal bus conditions
  - Decodes Baseband packets and provides decoding for 12 additional protocol levels
- Complies with Bluetooth v.1.1 specification
- 64 MB of physical data recording memory nets 32 MB of raw Bluetooth traffic
- Programmable real-time event triggering and traffic capture filtering
- CATC Trace graphical presentation of captured data with extensive customization options
- Adjustable recording size
- Adjustable trigger position
- Comprehensive search functions
- Accurate timestamping of packets
- Field upgradeable firmware and BusEngine™
- Software operates as a stand-alone Trace viewer
- Connects to the host computer through an available Type II PC Card slot
- One-year warranty and hotline customer support
- Traffic Generation

Traffic generation capability is provided by Merlin's Wand.

- Bluetooth™ BusEngine

  CATC's BusEngine™ Technology is at the heart of the new Merlin Mobile Analyzer. The revolutionary BusEngine core uses state-of-the-art EPLD technology and incorporates both the real-time recording engine and the configurable building blocks that implement data/state/error detection, triggering, capture filtering, external signal monitoring and event counting & sequencing. And like the flash-memory-based firmware that controls its operation, all BusEngine logic is fully field upgradeable, using configuration files that can be downloaded from the CATC Website.

2. Getting Started

This chapter describes how to install Merlin Mobile and its software, how to start Merlin Mobile, and how to set up the analyzer unit.

2.1 Installing Merlin Mobile

Merlin Mobile can be installed on any PC or laptop computer that uses the Windows 98 SE, Windows Me, Windows 2000, or Windows XP operating system and has a functioning PC Card slot.

Software Installation

The Merlin Mobile software can be installed from the installation CD-ROM or from installation files downloaded from the CATC website.

Install from CD-ROM

Step 1 Insert the Merlin Mobile installation CD-ROM into the CD-ROM drive of the computer that will be connected to the Merlin Mobile analyzer unit.

The autorun program should start automatically. If it doesn't start, use Windows Explorer or My Computer to navigate to the CD-ROM drive directory, double-click the file **autorun.exe**, and proceed to Step 2. If it still doesn't start, navigate to the \Software directory on the CD-ROM, double-click the file Setup.exe, and proceed to Step 3.

Step 2 Choose **Install Software** to start the setup program.

Step 3 Follow the on-screen instructions to complete the installation.

Install from installation download

Step 1 Select **Start > Run...** from the Windows taskbar and click the **Browse** button, then navigate to the Disk 1 directory of the Merlin Mobile installation download. Select the file **Setup.exe** and click Open.

Step 2 Follow the on-screen instructions to complete the installation.

2.2 Hardware Installation

Step 1 Insert the Merlin Mobile analyzer unit into the PC Card slot on the desktop or laptop computer that will be running the Merlin Mobile software.

Step 2 The New Hardware Wizard will automatically detect Merlin Mobile and will guide you through the rest of the installation.

2.3 Starting and Stopping Merlin Mobile

Starting the Application

Use one of the following procedures to start the Merlin Mobile application:

- Select **Start > Programs > CATC > CATC Merlin Mobile** from the Windows taskbar.
- In Windows Explorer or My Computer, navigate to the directory that contains Merlin Mobile, then double-click on the MerlinMobile.exe icon.

Exiting the Application

Any of the following actions will close the Merlin Mobile application:

- Click on the '**X**' in the upper right corner of the application window.
- Select **File > Exit** from the menu bar.
- Press **Alt + F4**.
- Double-click the **Merlin Mobile control icon** in the upper left corner of the application window.
- Click the Merlin Mobile control icon to access the Control menu and choose **Close**.

Starting the Analyzer Unit

The Merlin Mobile analyzer unit is powered on whenever it is connected to the host computer via the PC Card slot and the host computer is on. The analyzer will initialize itself and perform an exhaustive self-diagnostic test that lasts about five seconds.

Shutting Down the Analyzer Unit

On Windows 98 SE and Windows Me

- Shut down the Merlin Mobile unit by removing it from the PC Card slot or by shutting down the host computer.

On Windows 2000 and Windows XP

- Shut down the Merlin Mobile unit by shutting down the host computer.

  -OR-

- Use the Add/Remove Hardware Wizard to stop Merlin Mobile so that it may safely be removed from the PC Card slot.

2.4 Displaying Help

The Merlin Mobile application has a Help file that is useful as an on-screen reference. Access the Help file by choosing **Help > Help Topics...** from the menu bar.

2.5 Updating the BusEngine and Firmware

The BusEngine core is the heart of the Merlin Mobile analyzer. Using state-of-the-art PLD technology, it incorporates both the high speed recording engine and the configurable building blocks that implement data/state/error detections, triggering, capture filtering, external signal monitoring, and event counting and sequencing. Both the BusEngine program and the firmware that manage the internal microcontroller are fully field-upgradeable.

The most current BusEngine file and firmware file are included with the Merlin Mobile installation software and are automatically installed with the software. They are also updated anytime that the driver is updated.

2.6 Updating the Driver

The driver, BusEngine, and firmware are all automatically updated when the Merlin Mobile software is installed or upgraded.

To find out the current driver version number, please consult Merlin Mobile's Readme file.

The driver may also be manually updated. The steps below explain how to manually update the driver.

Note: The Merlin Mobile analyzer unit must be attached to the computer via the PC Card slot before updating the driver.

Updating the Driver on Windows 2000

Step 1 Select Start > Settings > Control Panel from the desktop taskbar, then double-click on Add/Remove Hardware in the Control Panel window.

The Add/Remove Hardware Wizard will open.

Step 2 Click Next.

Step 3 Choose "Uninstall/Unplug a device" and click Next.

Step 4 Choose "Unplug/Eject a device" and click Next.

Step 5 Select CATC Merlin Mobile Bluetooth Protocol Analyzer from the list of devices and click the Properties button.

The Properties window will open.

Step 6 Select the Driver tab in the Properties window and click Update Driver.

The Upgrade Device Driver Wizard will open.

Step 7 Click Next.

Step 8 Choose "Display a list of the known drivers for this device so that I can choose a specific driver." Then, click Next.

Step 9 Choose "Have disk" and click Next.

The Install from Disk window will open.

Step 10 Install from the Merlin Mobile installation CD-ROM:

Make sure that the installation CD is in the computer's CD-ROM drive, then click Browse and navigate to the \Software directory on the CD, or type the drive letter followed by \Software (e.g., "D:\Software") in the combo box. Click OK.

Install from a directory on the computer's hard drive:

Browse or enter the path to the Disk 1 directory of the Merlin Mobile installation, then click OK.

The Install from Disk window will close.

Step 11 Select CATC Merlin Mobile Bluetooth Protocol Analyzer from the list of devices in the Upgrade Device Driver Wizard and click Next.

Step 12 Click Next to install the driver.

Step 13 Click Finish to close the Wizard.

Step 14 Check the driver version on the Driver tab of the Properties window to make sure that the driver was successfully upgraded.

Step 15 Close the remaining open windows.

Updating the Driver on Windows 98 SE

Step 1 Select Start > Settings > Control Panel from the desktop taskbar, then double-click on System Properties in the Control Panel window.

The System Properties window will open.

Step 2 Select the Device Manager tab.

Step 3 Look in the CATC Analyzers directory and select CATC Merlin Mobile Bluetooth Protocol Analyzer.

or

Look in the Universal Serial Bus Controllers directory and select CATC Merlin Mobile Bluetooth Protocol Analyzer.

Step 4 Click the Properties button.

The Properties window will open.

Step 5 Select the Driver tab and click on the Update Driver button.

The Update Device Driver Wizard will open.

Step 6 Click Next.

Step 7 Choose "Search for a better driver than the one your device is using now." and click Next.

Step 8 Enter or browse to the location of the driver and click Next.

Step 9 Click Next to install the driver.

Note: If a message appears saying that Windows cannot locate the driver, click OK to close the message box and then enter or browse to the location of the driver to continue.

Step 10 Click Finish.

Step 11 Click the Driver File Details button to check the driver version and make sure that the driver was successfully upgraded.

Step 12 Close the remaining open windows.

Updating the Driver on Windows Me

Step 1 Select Start > Settings > Control Panel from the desktop taskbar, then double-click on System Properties in the Control Panel window.

The System Properties window will open.

Step 2 Select the Device Manager tab.

Step 3 Look in the CATC Analyzers directory and select CATC Merlin Mobile Bluetooth Protocol Analyzer.

or

Look in the Universal Serial Bus Controllers directory and select CATC Merlin Mobile Bluetooth Protocol Analyzer.

Step 4 Click the Properties button.

The Properties window will open.

Step 5 Select the Driver tab and click on the Update Driver button.

The Update Device Driver Wizard will open.

Step 6 Choose "Automatically search for a better driver." and click Next.

The Select Other Driver window will open.

Step 7 Select the newest driver and click OK.

The driver will install.

Step 8 Click Finish.

Step 9 Click the Driver File Details button to check the driver version and make sure that the driver was successfully upgraded.

Step 10 Close the remaining open windows.

Updating the Driver on Windows XP

Step 1 Select Start > Control Panel from the desktop taskbar, then double-click Performance and Maintenance.

Step 2 Double-click on System.

The System Properties window will open.

Step 3 Select the Hardware tab and click the Device Manager button.

The Device Manager window will open.

Step 4 Look in the CATC Analyzers directory and select CATC Merlin Mobile Bluetooth Protocol Analyzer.

or

Look in the Universal Serial Bus Controllers directory and select CATC Merlin Mobile Bluetooth Protocol Analyzer.

Step 5 Select Action > Update Driver... from the Device Manager menu bar.

The Hardware Update Wizard will open.

Step 6 Choose "Install from a list or specific location."

Step 7 Choose "Don't search" then click Have Disk.

Step 8 Enter or browse to the location of the driver and click OK.

Step 9 Select CATC Merlin Mobile Bluetooth Protocol Analyzer from the list and click Next.

The driver will install.

Step 10 Click Finish.

Step 11 Select Action > Properties from the Device Manager menu bar to check the driver version and make sure that the driver was successfully upgraded.

Step 12 Close the remaining open windows.

2.7 License Keys

A License Key is necessary to enable software maintenance in Merlin Mobile. License Keys must be obtained from CATC.

Update License

Follow these steps to install a license key:

Step 1 Select Help > Update License… from the menu bar.

The Update License dialog will come up.

Step 2 Enter the path and filename for the License Key or use the Browse button to navigate to the directory that contains the License Key. Select the .lic file, and then click Update Device.

License Information

Licensing information for Merlin Mobile may be viewed by selecting **Help > Display License Information...** from the menu bar. The License Information window will open, displaying the maintenance expiration and features data for Merlin Mobile.

2.8 Installing the HCI Probe

If you are planning to record HCI traffic, you will need to install an HCI probe.

The HCI Probe allows you to connect the analyzer software to a single IUT. If more IUTs are to be monitored (up to three) additional HCI Probes should be used.

The probe is composed of the following components:

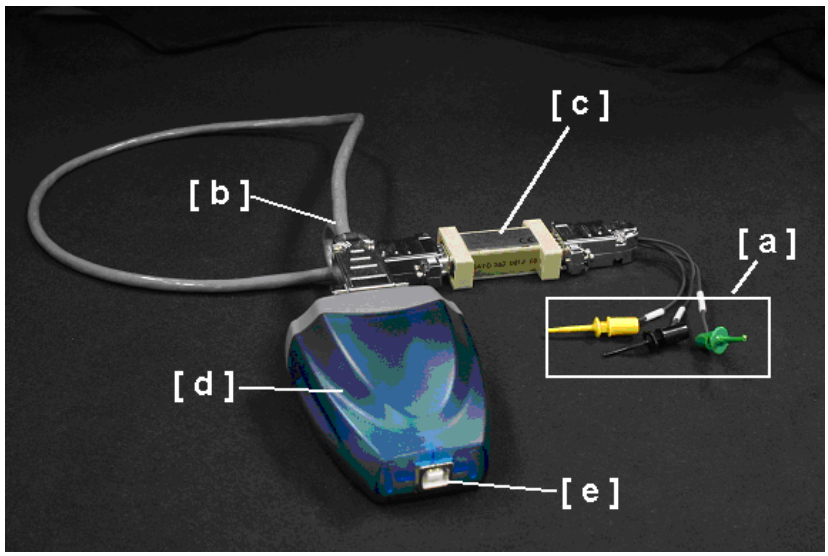
[a] HCITrace Probe Cable

[b] HCITrace RS232 Cable

[c] TTL to RS232 converter

[d] 2-port RS232 to USB converter

[e] USB cable



HCITrace Probe Cable

The HCITrace Probe Cable has three probes:

- 'Gnd' – Should be connected to the reference/ground wire
- 'Host' – Should be connected to the wire that carries the down-link traffic from the host to the controller.
- 'BTC'– Should be connected to the wire that carries the up-link traffic from the controller to the host.

HCITrace RS232 Cable

Has three DB-9 connectors:

- *RS-232/Probe* - Should be connected to the **HCITrace Probe Cable or to the** TTL to RS232 converter (depending whether the signal voltage in the IUT is TTL or RS-232).
- *COM A* - Should be connected to one of the serial inputs of the 2-port RS232 to USB converter.
- *COM B* - Should be connected to one of the other serial input of the 2-port RS232 to USB converter.

TTL to RS232 converter

Should be used only when the signal voltage in the IUT is TTL and not RS-232.

The DB-9 connector marked with 'TTL' should be connected to the **HCITrace Probe Cable.**

The DB-9 connector marked with 'RS-232' should be connected to the 'RS-232'/Probe connector of the **HCITrace RS232 Cable**.

2-port RS232 to USB converter -

This converter is used so the serial signals can be delivered to the host machine through a USB input.

USB cable –

Connects the **2-port RS232 to USB converter** to the Host machine USB port.

HCI Probe configurations

The HCI Probe can be used in two configurations:

- For monitoring UART level signals
- For monitoring RS232 level signals

Monitoring UART Level Signals

For monitoring RS232 level signals, the TTL to RS-232 converter should be used. To assemble the HCI probe for this configuration, perform the following steps. Refer to the photo and component list shown previously for references to components [a] through [e].

Step 1 Connect the DB-9 connector of the HCITrace Probe Cable [a] to the connector marked with 'TTL' in the TTL to RS-232 converter [c].

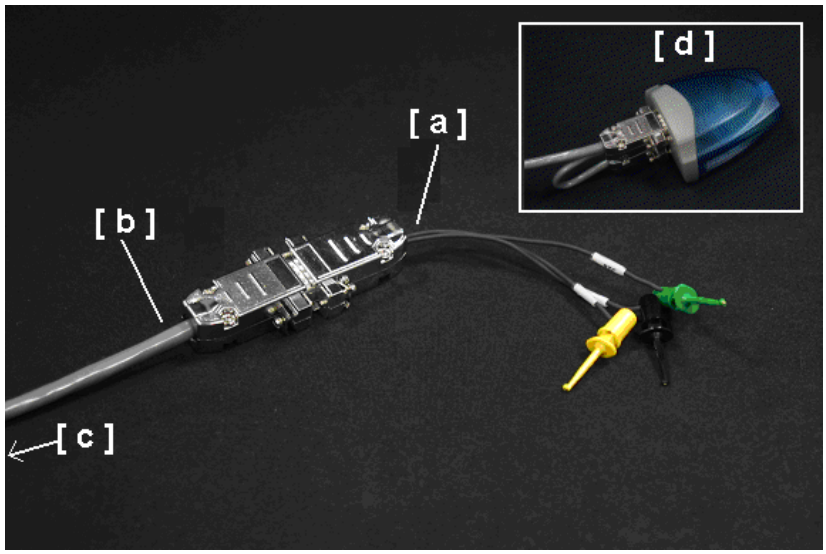
Step 2 Connect the DB-9 connector marked with 'RS-232' in the TTL to RS-232 converter [c] to the connector marked with ''RS-232/Probe'' in the HCITrace RS-232 Cable [b].

Step 3 Connect the connector marked with 'COM A' in the HCITrace RS-232 Cable [b] to 'Connector A' in the 2-port RS232 to USB converter [d].

Step 4 Connect the connector marked with 'COM B' in the HCITrace RS-232 Cable [b] to 'Connector B' in the 2-port RS232 to USB converter [d].

Step 5 Connect the USB cable to the USB connector of the 2-port RS232 to USB converter [e].

Monitoring RS232 level Signals



Legend for photo:

[a] HCI Probe Cable

[b] HCI Trace RS-232 Cable

[c] Connectors A and B on the other end of the HCI Trace RS-232 Cable

[d] Two-Port RS-232 to USB Converter

For monitoring RS232 level signals do not use the converter. To assemble the HCI probe for this configuration, perform the following steps:

Step 1 Connect the DB-9 connector of the HCITrace Probe Cable [a] to the connector marked with ''RS-232/Probe'' in the HCITrace RS-232 Cable [b].

Step 2 Connect the connector marked with 'COM A' in the HCITrace RS-232 Cable [c] to 'Connector A' in the 2-port RS232 to USB converter [d].

Step 3 Connect the connector marked with 'COM B' in the HCITrace RS-232 Cable [c] to 'Connector B' in the 2-port RS232 to USB converter [d].

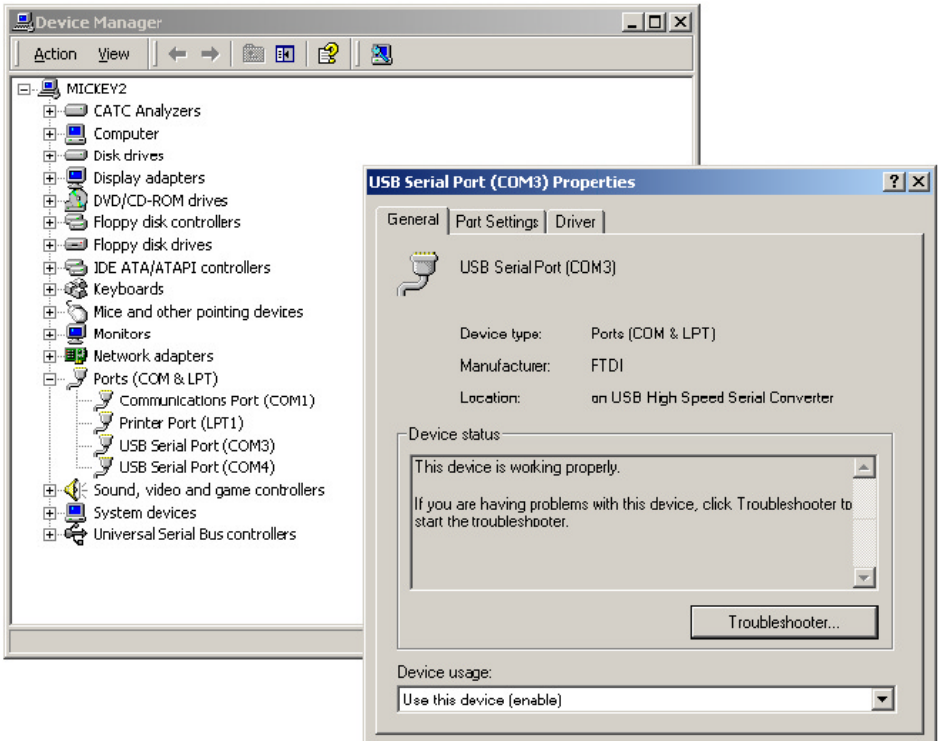
Step 4 Connect the USB cable [not shown] to the USB connector of the 2-port RS232 to USB converter [d].

2-port RS232 to USB converter

The 2-port RS232 to USB converter [d] allows the user to connect two serial connectors to the host machine via a single USB connection. When connected to the host machine the converter emulates two separate virtual COM ports that can be used as other real COM ports. Prior of using this converter as part of the HCI probe several drivers need to be installed. The drivers are provided on the installation CD-ROM in the HCI Probe\Drivers sub directory.

Once the converter is connected to a host machine the user is prompted to provide the place where the system can install the drivers from.

After installing the drivers two new COM ports are going to be available, as seen in the following snapshot of the Device Manager.



2.9 Your First Bluetooth Recording

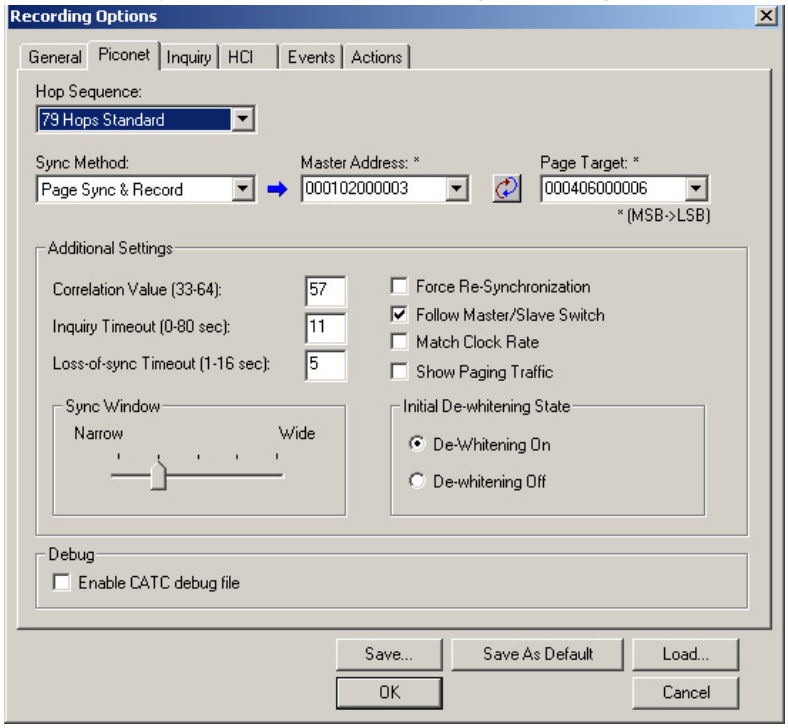
After installing and launching the software, you can test Merlin Mobile by synchronizing to a piconet and then recording the traffic. In this inquiry test, Merlin Mobile will issue a General Inquiry that asks local devices to identify themselves. Merlin Mobile then records the responses.

Step 1 Click the down-arrow on the Record button and select **Piconet**.

Step 2 From the menu, select **Record > Recording Options**.

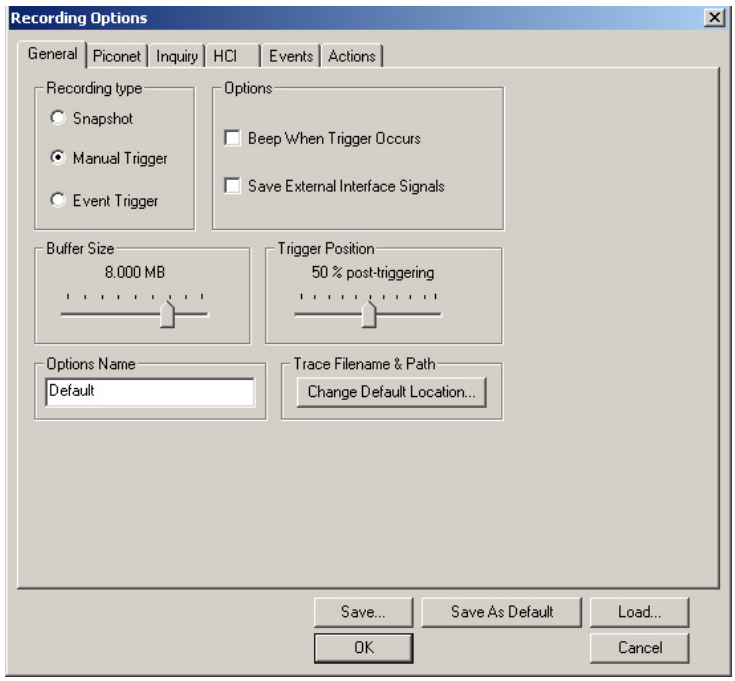
The following dialog box will open showing factory default settings. Merlin defaults to "**Page Sync & Record**." This setting tells Merlin Mobile to perform a General Inquiry and then collect sync

information from the specified slave device when the slave responds. Merlin Mobile then waits for the Master to begin paging the Slave devices. When paging begins, Merlin Mobile synchronizes to the Master and begins recording.

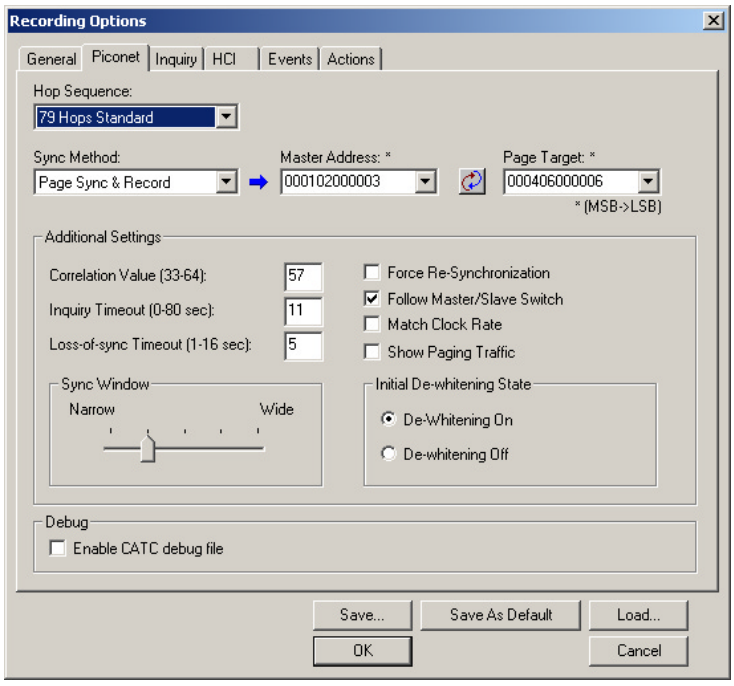


Step 3 Select the **General** tab.

The Recording Options dialog box opens showing factory default settings such as "manual trigger" and 8 MB buffer size. For the General Inquiry recording you are about to create, leave these settings unchanged.



For this recording, leave most of these settings unchanged. If you are recording a Hop Frequency that is not **79 Hops Standard**, you will need to select the appropriate standard from the **Hop Frequency** menu below.

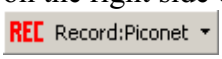


Step 4 Click **OK** to close the Recording Options window and activate the recording options you selected.

At this point, Merlin Mobile will be ready to record.

Inquiry Recording

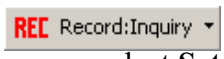
Merlin Mobile can also record an inquiry process where the Merlin Mobile performs a general inquiry and asks local devices to identify themselves.

Step 1 Click the down-arrow on the right side of the **Record:Piconet** button on the toolbar 

.

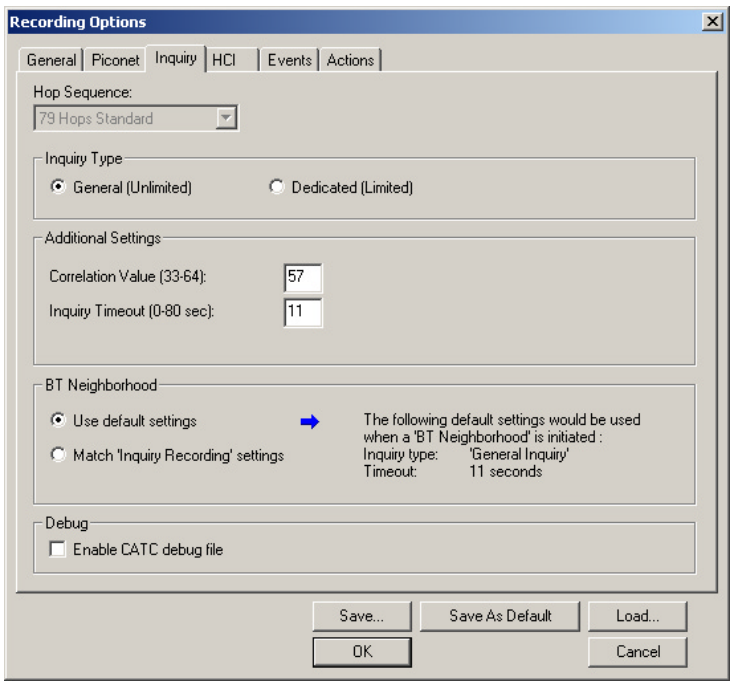
A sub-menu appears with options for **Piconet Recording Mode**, and **Inquiry Recording Mode**.

Step 2 Select **Inquiry Recording Mode**.

The button changes appearance and shows the label **Record: Inquiry** 

Step 3 From the menu, select **Setup** > **Recording Options**.

The Recording Options dialog opens with the **Inquiry** page displaying.



Step 4 If desired, make any changes to the options, then click **OK.**

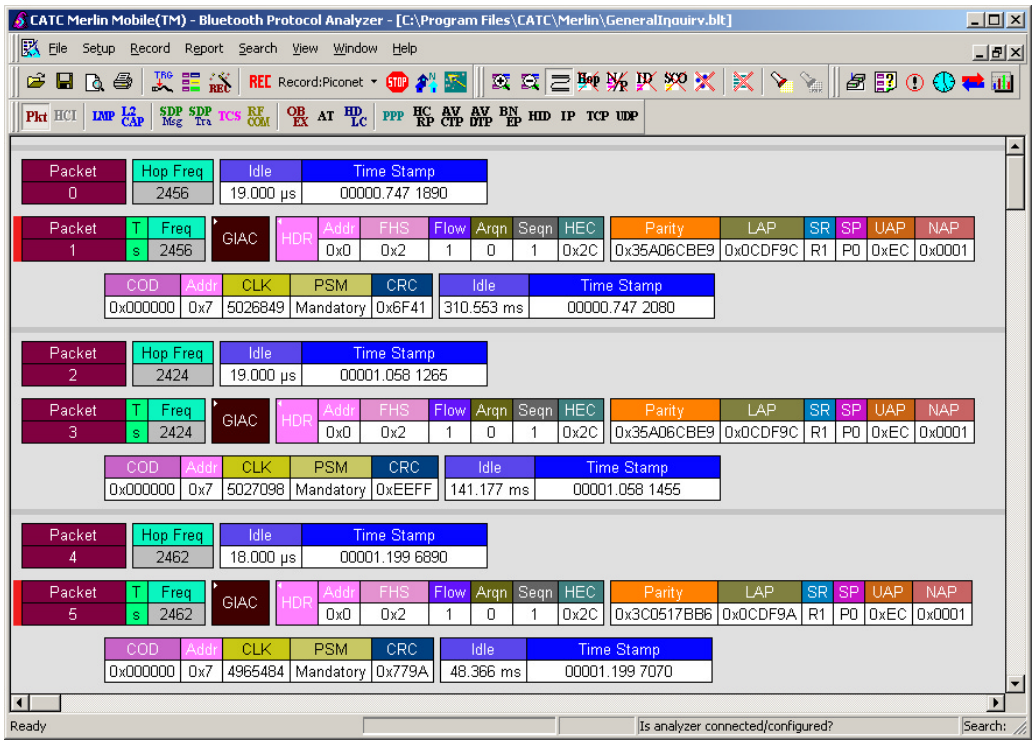
Step 5 Click the

button (i.e. the button itself, and not the down-arrow.)

Merlin Mobile starts to record the Bluetooth traffic immediately using the settings from the Piconet page in the Recording Options dialog. The Bluetooth Inquiry process will proceed for whatever amount of time is set for creating an Inquiry action (0 to 80 seconds). After the inquiry time has elapsed, the analyzer will uploads the data and displays the packets.

After a few moments, the recording will terminate and the results will display. The screen should look like the sample recording below which shows the FHS packets generated during the Inquiry process.

When the recording session is finished, the bus traffic is saved to the hard drive as a file named **data.tfb** or whatever name you assign as the default filename. While the file is being saved, you should see a brown progress bar at the bottom of the screen. When the bar turns white, it indicates that the data has been saved to disk.


CATC Merlin Mobile(TM) - Bluetooth Protocol Analyzer - [C:\Program Files\CATC\Merlin\GeneralInquiry.blt]
File Setup Record Report Search View Window Help
Record:Piconet
Packet 0 Hop Freq 2456 Idle 19.000 µs Time Stamp 00000.747 1890
Packet 1 T s Freq 2456 GIAC HDR Addr 0x0 FHS 0x2 Flow 1 Arqn 0 Seqn 1 HEC 0x2C Parity 0x35A06CBE9 LAP 0x0CDF9C SR R1 SP P0 UAP 0xEC NAP 0x0001
COD 0x000000 Addr 0x7 CLK 5026849 PSM Mandatory CRC 0x6F41 Idle 310.553 ms Time Stamp 00000.747 2080
Packet 2 Hop Freq 2424 Idle 19.000 µs Time Stamp 00001.058 1265
Packet 3 T s Freq 2424 GIAC HDR Addr 0x0 FHS 0x2 Flow 1 Arqn 0 Seqn 1 HEC 0x2C Parity 0x35A06CBE9 LAP 0x0CDF9C SR R1 SP P0 UAP 0xEC NAP 0x0001
COD 0x000000 Addr 0x7 CLK 5027098 PSM Mandatory CRC 0xEEFF Idle 141.177 ms Time Stamp 00001.058 1455
Packet 4 Hop Freq 2462 Idle 18.000 µs Time Stamp 00001.199 6890
Packet 5 T s Freq 2462 GIAC HDR Addr 0x0 FHS 0x2 Flow 1 Arqn 0 Seqn 1 HEC 0x2C Parity 0x3C0517BB6 LAP 0x0CDF9A SR R1 SP P0 UAP 0xEC NAP 0x0001
COD 0x000000 Addr 0x7 CLK 4965484 PSM Mandatory CRC 0x779A Idle 48.366 ms Time Stamp 00001.199 7070
Ready
Is analyzer connected/configured?
Search:

Step 6 To save a current recording for future reference, Select **Save As** under **File** on the Menu Bar.

OR

Click on the Tool Bar.

You see the standard **Save As** screen.

Step 7 Give the recording a unique name and save it to the appropriate directory.

3. Software Overview

3.1 The Main Display Windows

While some of the analyzer's Main Display window options are familiar, many contain options specific to the analyzer program.

Table 1: Main Display Pull-Down Windows

Menu	Function
File	
Open…	Opens a file
Close	Closes the current file
Save As…	Saves all or a specified range of packets from the current file with a specified name
Print…	Prints part or all of the current traffic data file
Print Preview	Produces an on-screen preview before printing
Print Setup…	Sets up your current or new printer
Edit Comment…	Creates or edits the Trace file comment field
Export » Packets to Text (Packet View Format)	Saves all or part of a trace to a text file
Export » Packets to CSV Text	Saves all or part of a trace to a Comma Separated Values (CSV) file suitable for viewing in a spreadsheet application
Export>>Audio Streams	Saves audio data into a file. Presents options for setting the Audio Source format, Output File format, Stream Direction, and Output Sampling
Last File	Lists the last files that were opened
Exit	Exits the Merlin program
Setup	
Display Options	Provides the control of various display options such as color, formats, and filters.
Recording Options	Opens a dialog box with checkboxes and drop-down menus for setting up a recording.
Recording Wizard	Starts a sequence of interactive dialog boxes that configures Merlin for a recording. This utility provides an alternative to the Recording Options dialog box.
Analyzer	Allows the operator to reset the Analyzer or update the BusEngine and Firmware.
Record	
Start	Causes the Analyzer to begin recording Bluetooth activity.
Stop	Causes the Analyzer to stop recording.

Menu	Function
Recording Mode	Presents a drop-down menu with options for setting the analyzer's recording mode: ***Piconet Recording Mode*** -- Causes Merlin to monitor and record piconet traffic. Merlin records the traffic data as specified in the Recording Options, then uploads the data as a Trace file when the recording is complete. ***Inquiry Recording Mode*** -- Causes Merlin to perform an inquiry to detects and records Bluetooth devices within range. After completing the recording, Merlin uploads the trace to the PC and saves it as a Trace file. *IUT: HCI Recording Mode* -- Causes the Merlin software to record HCI traffic from the IUT. In this mode, the Merlin software on the host PC directly records IUT traffic without first going through the analyzer.
BT Neighborhood Inquiry	Displays Bluetooth Address and clock frequency for devices in range. The expected Bluetooth clock frequency is 3200 Hz +/- 250 ppm.
Report	
File Information	Details such information about the recording as number of packets and triggering setup.
Error Summary	Displays an error summary of the current trace file and allows you to go to a specific packet, and save the error file to a uniquely named file.
Timing Calculation	Starts the calculator dialog for calculating various timing and bandwidth parameters in the recording file.
Traffic Summary	Details the number and type of packets were transferred during the recording, as well as message-level statistics.
Search	
Go to trigger	Positions the display to show the first packet that follows the trigger event.
Go to Packet/Message/ Protocol ...	Positions the display to the indicated packet, LMP/L2CAP message, or Protocol Message (RFCOMM, TCS, or SDP protocols).
Go to Marker »	Positions the display to a previously marked packet.
Go to »	Enables quick searching for specific events using a cascade of pop-up windows.
Find	Allows complex searches.
Find Next	Repeats the previous Find operation. Can also use F3 to find next.
Search Direction	Allows you to specify a forward or backward search of a trace file.

Menu	Function
View	
Toolbars	Presents a sub-menu with options for displaying/hiding the toolbars and an option called Customize which allows the menus and toolbars to be customized or reset to factory default.
Status Bar	Switches display of the Status Bar on or off.
Unhide Cells >	Presents a menu of currently hidden cells. Allows you to unhides any cells that were hidden through the Display Options dialog box (View > Display Options > Color/Format/Hiding)
Zoom In	Increases the size of the displayed elements.
Zoom Out	Decreases the size of the displayed elements.
Wrap	Allows the display to wrap.
Device List	Displays a list of discovered Bluetooth devices and allows you to add and delete devices and security settings by selecting the device, pressing the security button, and modifying the settings.
Real-time Statistics	Opens a dialog box with a graphical summary of the traffic currently being recorded by the Analyzer. Real-time monitoring allows continuous monitoring and displaying of traffic and related statistical dada in a piconet. This processed data is displayed in a set of configurable graphs.
Decoding Assignments	Lists current L2CAP decoding assignments.
L2CAP Connections	Lists current L2CAP connections.
RFCOMM Channel Assignments	Lists current RFCOMM assignments.
Levels	Presents a menu of display levels. This menu replicates the Decode/Display buttons in the toolbar such as Packets, L2CAP, TCS etc.)
Window	
New Window	Switches display of the Tool Bar on or off.
Cascade	Displays all open windows in an overlapping arrangement.
Tile	Arranges multiple trace windows as a series of strips across the main display area or as a series of side-by-side tiles.
Arrange Icons	Arranges minimized windows at the bottom of the display.
Windows	Displays a list of open windows.

Help	
Online Help	Displays Help topic associated with current Merlin window.
Help Topics...	Displays online help.
Update License...	Opens a dialog box for entering license key information for the analyzer.
Display License Information...	Displays current license information for the analyzer.
About Merlin...	Displays version information about Merlin.

3.2 Toolbar

The Tool Bar provides access to the most popular program functions. Tool tips describe icon functionality as the mouse arrow is moved over the icon/item.

Open file

Save As

Preview

Print…

Setup Record Options

REC Record:Piconet Start Recording - presents options for recording piconet, inquiry, or IUT:HCI traffic

Stop Recording

Execute manual trigger. Causes analyzer to trigger end of recording.

Start Recording Wizard

View/Hide L2CAP Message Level

View/Hide SDP Message Protocol Level

View/Hide SDP Transaction Protocol Level

View/Hide TCS Protocol Level

View/Hide RFCOMM Protocol Level

View/Hide OBEX Protocol Level

View AT Commands Protocol Level

View/Hide HDLC Protocol

View/Hide PPP

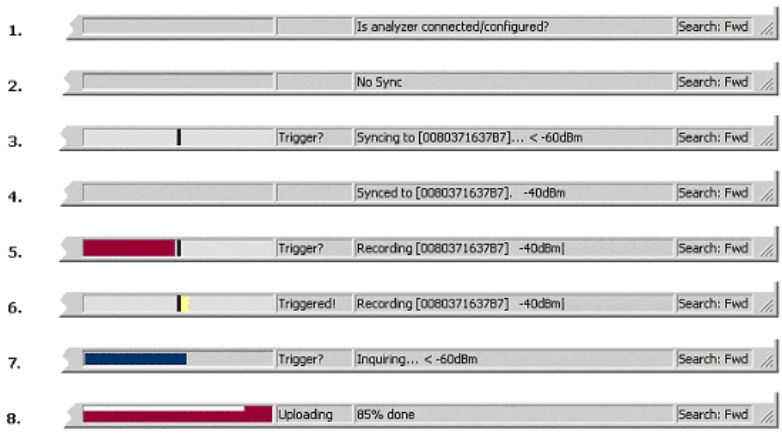
	Bluetooth Neighborhood. Performs an inquiry and then lists the local devices that it discovered		View/Hide HCRP
	Start Merlin's Wand		View/Hide AVCTP
	Setup Display Options		View/Hide AVDTP
	Zoom In		View/Hide BNEP Protocol
	Zoom Out		View HID Protocol Layer
	Wrap		View IP Protocol Layer
	Hide Frequency Hops		View TCP Protocol Layer
	Hide Nulls & Polls		View UDP Protocol Layer
	Hide ID Packets		Display device list
	Hide Voice (SCO) Packets		File Information Report
	Hide devices that were specified in the Display Options dialog box		Error Summary
	Hide Unassociated Traffic		Timing Calculations
	Complex Find		Traffic Summary
	Find Next		Display Bus Utilization graph
	View Packet Level (Baseband)		Display Real-Time Statistics
	View/Hide LMP Message Level		View HCI Protocol layer.

3.3 Status Bar

The Status Bar is located at the bottom of the main display window. Depending on the current activity, the bar can be divided into as many as four segments. The figure below demonstrates the various displays in the status bar.

Recording Progress

When you begin recording, the left-most segment of the Status Bar displays a Recording Progress Indicator. The following figure displays the various indications of the status bar:



Status Bar Position Definitions:

The following numbered definitions correspond to the number labels on the above status bars.

1 Analyzer is not connected or not configured.

2 Idle mode: Analyzer is connected to the host machine, but is not doing any attempts to synchronize to a piconet nor record Bluetooth traffic.

3 Analyzer is trying to synchronize to the piconet with the master device that has BD_Address 00837163787.

4 Analyzer is synchronized to the piconet with the master device that has BD_Address 00837163787.

5 Analyzer is recording the traffic of the piconet with the master device that has BD_Address 00837163787. However, no triggering occurred.

6 A trigger event occurred, and the analyzer is recording the traffic of the piconet with the master device that has BD_Address 00837163787. However, no triggering occurred.

7 Analyzer is performing a BT Neighborhood action, where it makes inquiries for Bluetooth devices.

8 Merlin application uploads recorded data from the analyzer at the end of a recording session.

As recording progresses, the Progress Indicator changes to reflect the recording progress graphically:

- In the Progress Indicator, a black vertical line illustrates the location of the Trigger Position you selected in Recording Options.
  - Pre-Trigger progress is displayed in the field to the left of the Trigger Position in the before-Trigger color specified in the Display Options.
  - When the Trigger Position is reached, the progress indicator wiggles as it waits for the trigger.
  - After the trigger occurs, the field to the right of the Trigger Position fills in the post-Trigger color specified in the Display Options.
  - When recording is complete, the upper half of the progress indicator fills in white, indicating the progress of the data upload to the host computer.

You should be aware of two exceptional conditions:

- If a Trigger Event occurs during the before-Trigger recording, the before-Trigger color changes to the after-Trigger color to indicate that not all the expected data was recorded pre-Trigger.
- When you click **Stop** before or after a Trigger Event, the Progress Bar adjusts accordingly to begin uploading the most recently recorded data.

The Progress Bar fills with color in proportion to the specified size and actual rate at which the hardware is writing and reading the recording memory. However, the Progress Indicator is normalized to fill the space within the Status Bar.

Recording Status

During recording activity, the current Recording Status is temporarily displayed in the next segment. When you activate the **Record** function, this segment flashes one of the following messages (depending on the selected Recording Options):

- Trigger?
- Triggered!
- Uploading

After recording stops,

— The flashing message changes to **Uploading data–*x*% done** (**x%** indicates the percentage completion of the data uploading process).

— The traffic data is copied to disk (overwriting any previous version of this file) using the default file name **data.tfb** or a new name specified in the Recording options.

To abort the upload process,

Click in the Tool Bar.

You are prompted to choose whether to keep the partially uploaded data or to throw it away.

When the data is saved, the Recorded Data file appears in the main display window and the Recording Status window is cleared.

- If the recording resulted from a Trigger Event, the first packet following the Trigger (or the packet that caused the Trigger) is initially positioned second from the top of the display.
- If the recording did not result from a Trigger Event, the display begins with the first packet in the traffic file.

Analyzer Status

The third segment in the status bar displays analyzer status. The status will display one of the following:

No Sync - the system is not synced to any piconet

Inquiring... - The system is performing an Bluetooth Inquiry

Syncing to [XXX]... -- The system is attempting to synchronize to a piconet where the device with BD_Address XXX is the master.

Synced to [XXX] - The system is synchronized to a piconet where the device with BD_Address XXX is the master.

Recording [XXX] - system is recording the Bluetooth traffic of the piconet where the device with BD_Address XXX is the master.

After the analyzer has synchronized to the Bluetooth piconet under observation, the Status Bar will display activity bars and the strength (in dBm) of the radio signal that Merlin is receiving. The activity bars will increase or decrease with activity. The signal strength readings will display as five possible values:

- below -60 dBm
- - 60 dBm
- - 50 dBm
- - 40 dBm

- above - 40 dBm

The valid range for a signal is between -60 and - 40 dBm

Search Status

The rightmost segment displays the current search direction: **Fwd** (forward) or **Bwd** (backward).

Zoom In

Zoom In increases the size of the displayed elements, allowing fewer (but larger) packet fields per screen.

- Click on the Tool Bar.

Zoom Out

Zoom Out decreases the size of the displayed elements, allowing more (but smaller) packet fields per screen.

- Click on the Tool Bar.

3.4 Tool Tips

Throughout the application, tool tips provide useful information.

To display a tool tip, position the mouse pointer over an item. The tool tip displays in a short moment if present. Tool tips can also be found over the Tool Bar and in areas of the packet view screen.

3.5 Merlin Analyzer Keyboard Shortcuts

Several frequently-used operations are bound to keyboard shortcuts.

Table 2: Keyboard Shortcuts

Key Combination	Operation	Key Combination	Operation
Ctrl+O	Open file	Ctrl+P	Print...
Ctrl+Home	Jump to First packet	Ctrl+End	Jump to Last packet
Ctrl+F	Search Forward	Ctrl+B	Search Backward
F3	Find Next	Ctrl+L	Search for Loss of Sync
Shift+I	Goto ID packet	Shift+R	Goto Freq Hop packet
Shift+P	Goto Poll packet	Shift+N	Goto Null packet
Shift+M	Goto DM1 packet	Shift+F	Goto FHS packet
Shift+1	Goto HV1 packet	Shift+H	Goto DH1 packet
Shift+3	Goto HV3 packet	Shift+2	Goto HV2 packet
Shift+A	Goto AUX1 packet	Shift+V	Goto DV packet
Shift+5	Goto DH3 packet	Shift+4	Goto DM3 packet

Key Combination	Operation
Shift+7	Goto DH3 packet
Shift+S	Search for Soft Error

Key Combination	Operation
Shift+6	Goto DM5 packet
Shift+E	Search Error

5. Recording Wizard

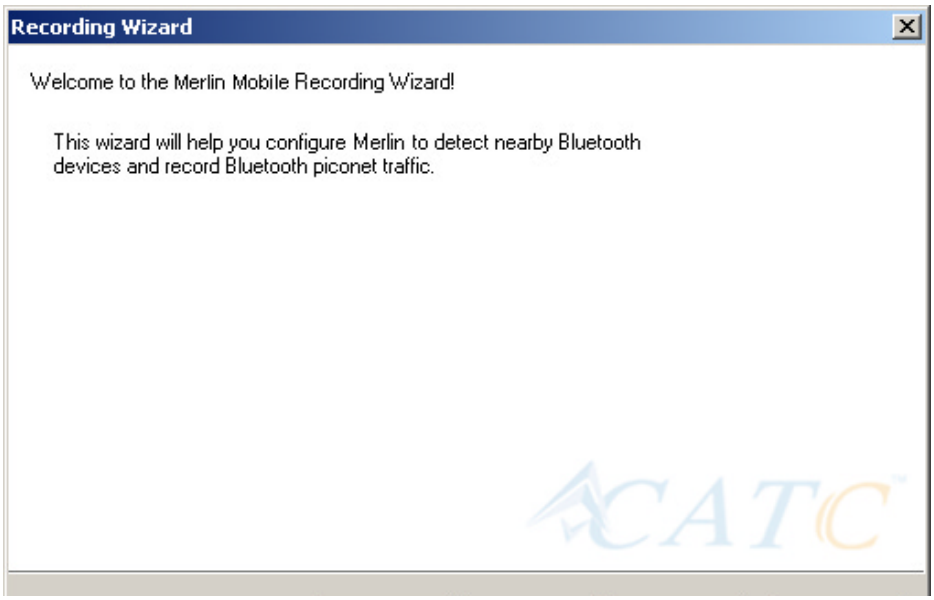
Recording Wizard is an interactive utility that presents a series of user-friendly dialog boxes for setting up a recording session. Recording Wizard serves as an alternative method of configuring the Recording Options dialog box. When you are finished using the Wizard, you can view your settings in the Recording Options window. By providing data to the prompts in the Wizard's dialog boxes, you configure Merlin Mobile for a recording session.

Starting Recording Wizard

To start the **Recording Wizard**,

- Click on the Tool Bar or select **Recording Wizard** under **Setup** on the Menu Bar.

You see the **Recording Options** window:

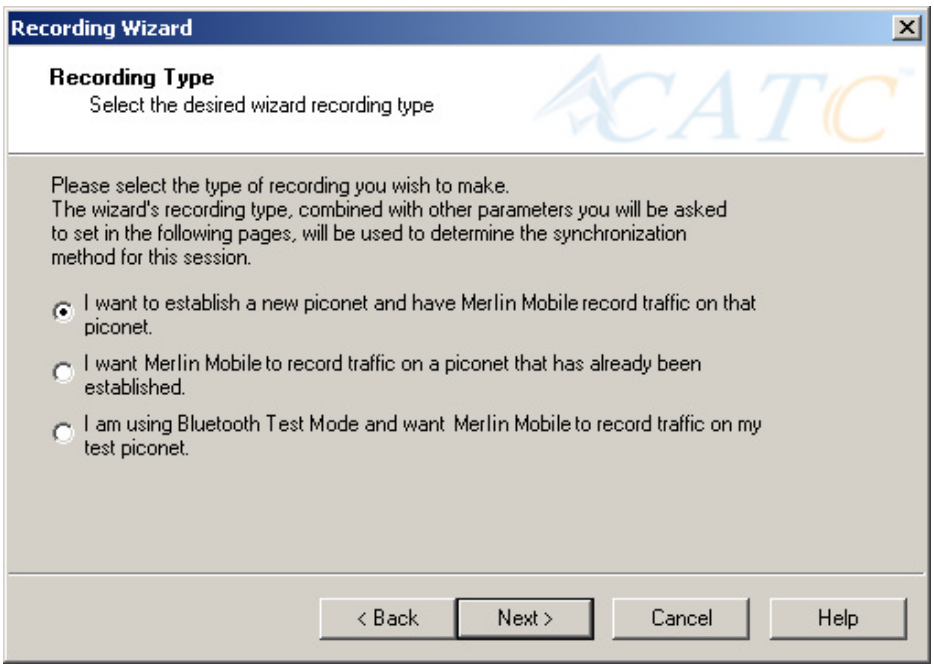

Recording Wizard
Welcome to the Merlin Mobile Recording Wizard!
This wizard will help you configure Merlin to detect nearby Bluetooth devices and record Bluetooth piconet traffic.
CATC

The **Recording Options** window has three buttons marked **Next**, **Back**, and **Cancel** that allow you to move forward or backward through the wizard or to cancel the wizard.

To begin advancing through the wizard,

- Click **Next** to see the options for the three types of recordings that the Recording Wizard can make.

The Wizard advances to the next screen which presents three options:


Recording Wizard
Recording Type
Select the desired wizard recording type
Please select the type of recording you wish to make.
The wizard's recording type, combined with other parameters you will be asked to set in the following pages, will be used to determine the synchronization method for this session.
I want to establish a new piconet and have Merlin Mobile record traffic on that piconet.
I want Merlin Mobile to record traffic on a piconet that has already been established.
I am using Bluetooth Test Mode and want Merlin Mobile to record traffic on my test piconet.
< Back
Next >
Cancel
Help

- **I want to establish a new piconet and have Merlin Mobile record traffic on that piconet.**

This option causes Merlin Mobile to perform an Inquiry so it can discover local devices and then establish a new piconet and record the piconet traffic.

- **I want Merlin Mobile to record traffic on a piconet that has already been established.**

This option lets Merlin Mobile record traffic from an already established piconet.

- **I am using Bluetooth Test Mode and want Merlin Mobile to record traffic on my test piconet.**

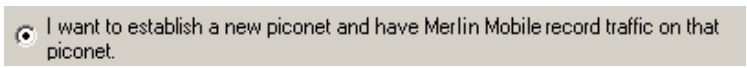
This option lets Merlin Mobile create either a single frequency range recording of a range that you specify or create a recording of a limited hop frequency range consisting of 5 frequency hops.

5.1 Recording a Traffic on a New Piconet

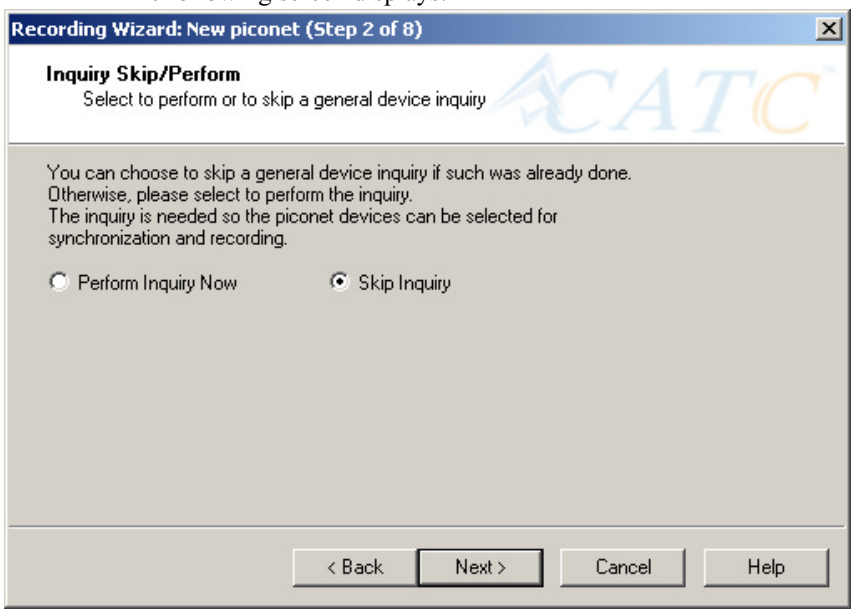
The **New Piconet** option shown in the previous screen presents users with the means of recording the traffic from a new piconet. This option will cause a sequence of screens to prompt you for information such as the piconet Master address.

The following steps shows you how to configure Merlin Mobile to record a new piconet.

Step 1 From the screen shown in the previous screenshot, select the first option: **I want to establish a new piconet and have Merlin Mobile record traffic on that piconet**, then press **Next**.



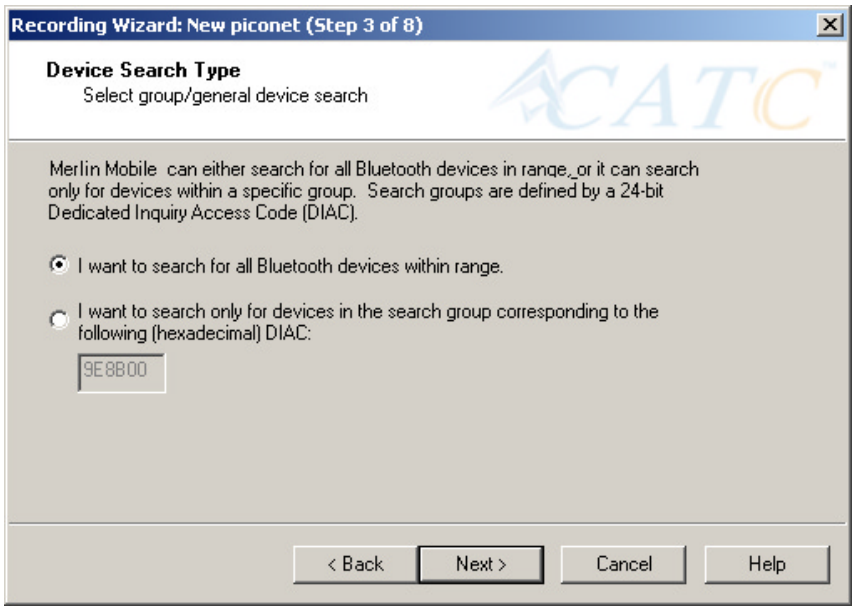
The following screen displays.


Recording Wizard: New piconet (Step 2 of 8)
Inquiry Skip/Perform
Select to perform or to skip a general device inquiry
You can choose to skip a general device inquiry if such was already done.
Otherwise, please select to perform the inquiry.
The inquiry is needed so the piconet devices can be selected for synchronization and recording.
Perform Inquiry Now
Skip Inquiry
< Back
Next >
Cancel
Help

Step 2 Select **Perform Inquiry Now**, then press **Next**.

Selecting **Perform Inquiry Now** will cause Merlin Mobile to perform a General Inquiry and collect addresses and other details about local Bluetooth devices. If you already have address information for your Bluetooth devices you can choose **Skip Inquiry**. Choosing **Skip Inquiry** will cause the Recording Wizard to advance to Step 6. If you are not sure what option to select, choose **Perform Inquiry Now**.

The following screen will display.


Recording Wizard: New piconet (Step 3 of 8)
Device Search Type
Select group/general device search
Merlin Mobile can either search for all Bluetooth devices in range, or it can search only for devices within a specific group. Search groups are defined by a 24-bit Dedicated Inquiry Access Code (DIAC).
I want to search for all Bluetooth devices within range.
I want to search only for devices in the search group corresponding to the following (hexadecimal) DIAC:
9E8B00
< Back
Next >
Cancel
Help

You will see two options:

- **I want to search for all Bluetooth devices within range**

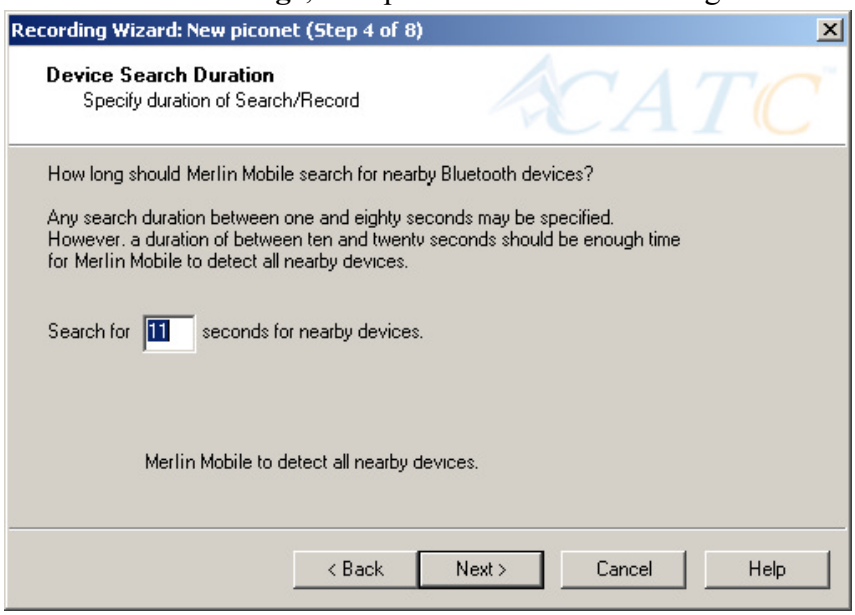
This option will cause Merlin Mobile to search for all Bluetooth devices that are in range and ready to transmit and receive data (i.e., in *Inquiry Scan Mode*)

- **I want to search only for devices corresponding to the following (hexadecimal) DIAC:**

This option will cause Merlin Mobile to search for the class of devices that you specify in the DIAC text box. DIAC stands for *Device Inquiry Access Code*. Values are entered in hexadecimal format. You can get DIAC values from the Bluetooth Specification.

Step 3 Select the first option: **I want to search for all Bluetooth devices**

within range, then press **Next**. The following screen will display.


Recording Wizard: New piconet (Step 4 of 8)
Device Search Duration
Specify duration of Search/Record
How long should Merlin Mobile search for nearby Bluetooth devices?
Any search duration between one and eighty seconds may be specified.
However. a duration of between ten and twenty seconds should be enough time
for Merlin Mobile to detect all nearby devices.
Search for 11 seconds for nearby devices.
Merlin Mobile to detect all nearby devices.
< Back
Next >
Cancel
Help

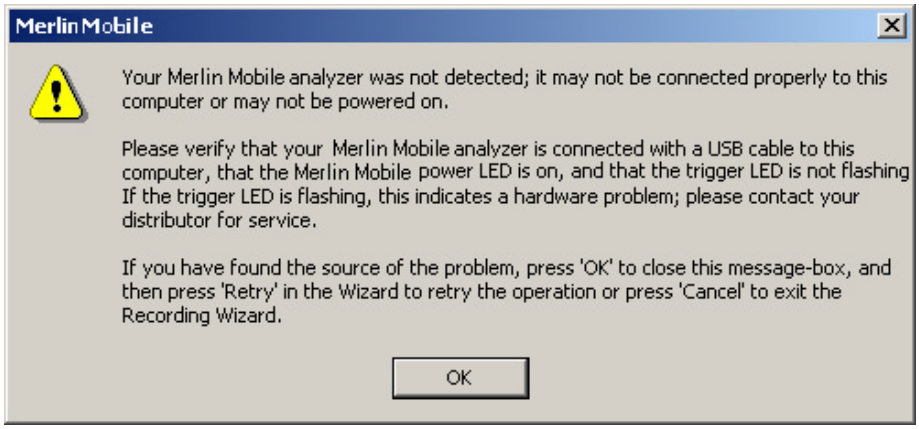
You will see two options:

Step 4 In the text box, enter the length of time you want Merlin Mobile to search for nearby devices.

The default value is **11**. If you do not sure what time value to enter, use the default value.

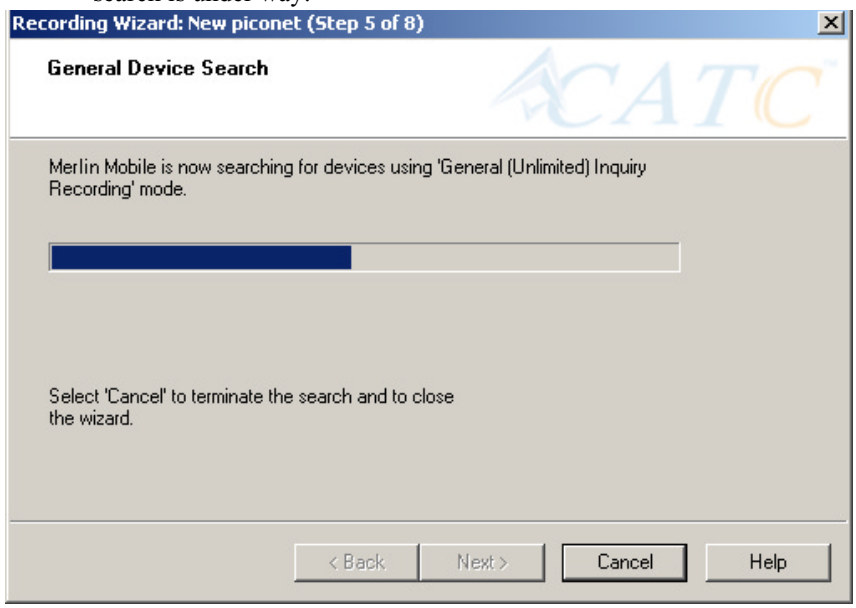
Step 5 Press **Next**.

Before the Inquiry, Merlin Mobile tests the hardware connection. In the case of failure, the following screen will display.

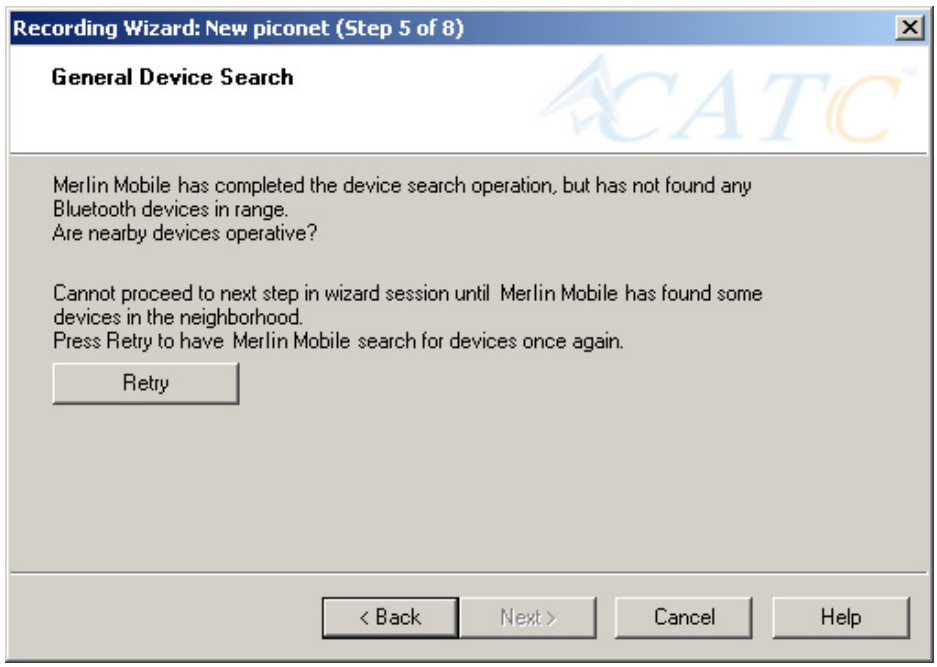

Merlin Mobile
Your Merlin Mobile analyzer was not detected; it may not be connected properly to this computer or may not be powered on.
Please verify that your Merlin Mobile analyzer is connected with a USB cable to this computer, that the Merlin Mobile power LED is on, and that the trigger LED is not flashing If the trigger LED is flashing, this indicates a hardware problem; please contact your distributor for service.
If you have found the source of the problem, press 'OK' to close this message-box, and then press 'Retry' in the Wizard to retry the operation or press 'Cancel' to exit the Recording Wizard.
OK

Clicking **OK** will close the message box.

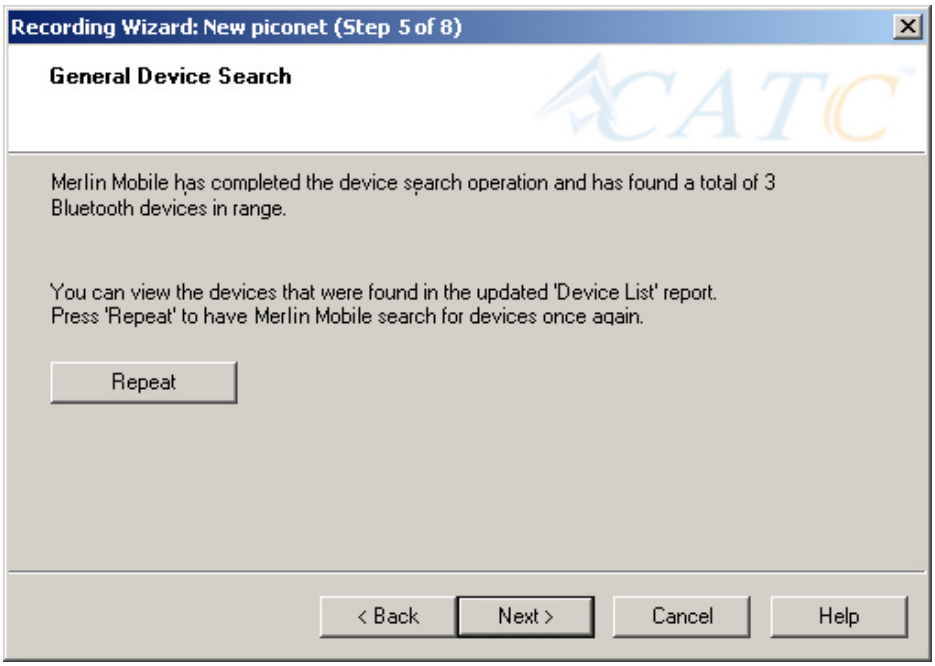
If Merlin Mobile passes the hardware test, it will search for devices. The Recording Wizard will display a progress bar and a message telling you that a search is under way:


Recording Wizard: New piconet (Step 5 of 8)
General Device Search
Merlin Mobile is now searching for devices using 'General (Unlimited) Inquiry Recording' mode.
Select 'Cancel' to terminate the search and to close the wizard.
< Back
Next >
Cancel
Help

If no device is found, the Recording Wizard will display the following screen:

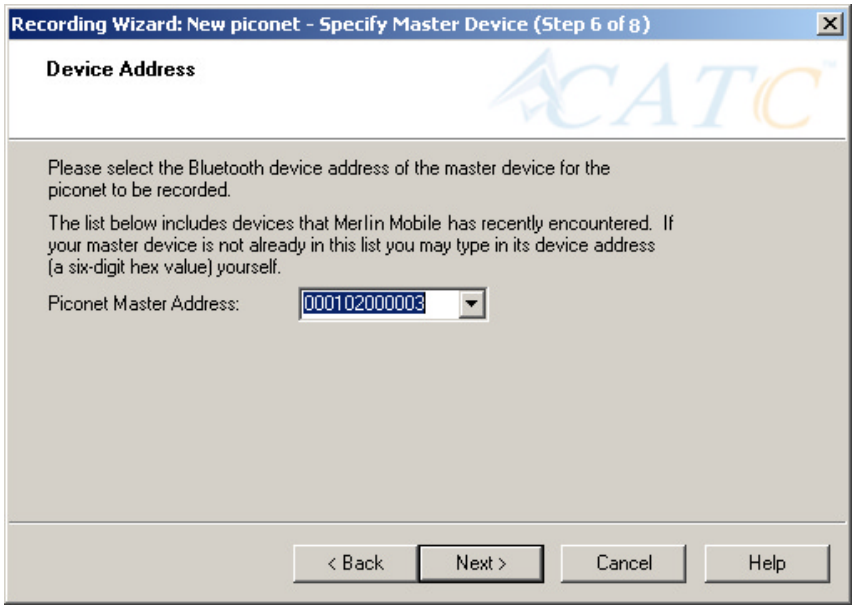

Recording Wizard: New piconet (Step 5 of 8)
General Device Search
Merlin Mobile has completed the device search operation, but has not found any Bluetooth devices in range.
Are nearby devices operative?
Cannot proceed to next step in wizard session until Merlin Mobile has found some devices in the neighborhood.
Press Retry to have Merlin Mobile search for devices once again.
Retry
< Back
Next >
Cancel
Help

If devices found, the Recording Wizard will display the following screen:


Recording Wizard: New piconet (Step 5 of 8)
General Device Search
Merlin Mobile has completed the device search operation and has found a total of 3 Bluetooth devices in range.
You can view the devices that were found in the updated 'Device List' report.
Press 'Repeat' to have Merlin Mobile search for devices once again.
Repeat
< Back
Next >
Cancel
Help

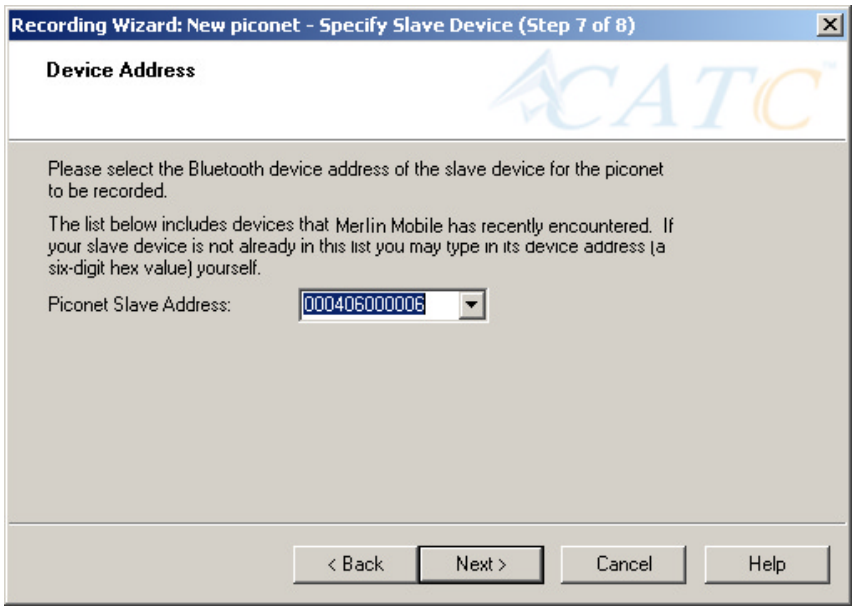
Step 6 Press **Next**.

The following window will display:


Recording Wizard: New piconet - Specify Master Device (Step 6 of 8)
Device Address
Please select the Bluetooth device address of the master device for the piconet to be recorded.
The list below includes devices that Merlin Mobile has recently encountered. If your master device is not already in this list you may type in its device address (a six-digit hex value) yourself.
Piconet Master Address:
000102000003
< Back
Next >
Cancel
Help

Step 7 Select from the drop-down menu the hexadecimal address for your Master device. If you do not see your device's address, you may type it into the text box yourself.

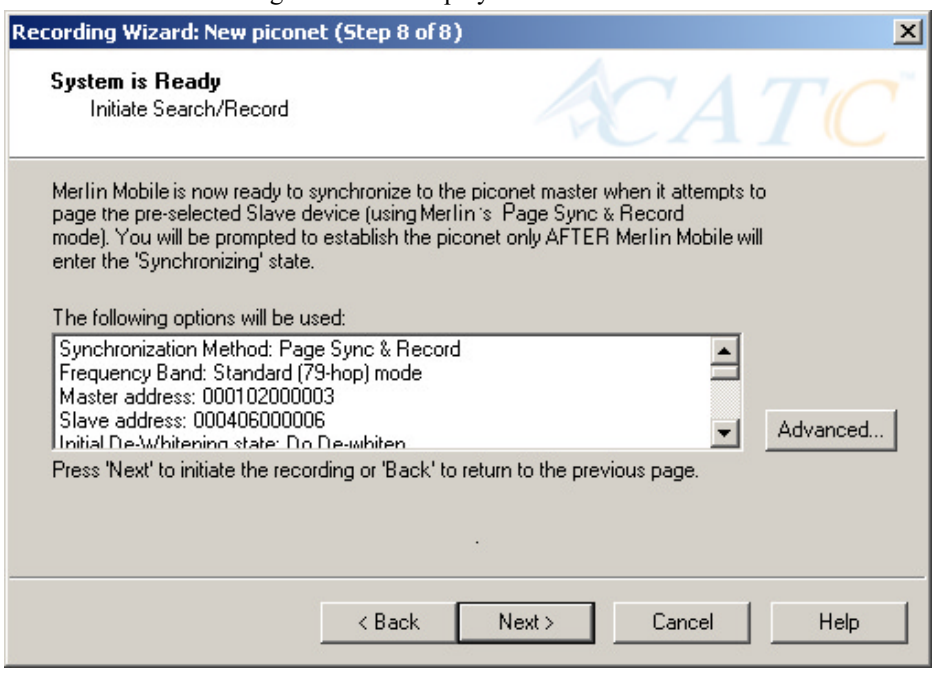
The following window will display:


Recording Wizard: New piconet - Specify Slave Device (Step 7 of 8)
Device Address
Please select the Bluetooth device address of the slave device for the piconet to be recorded.
The list below includes devices that Merlin Mobile has recently encountered. If your slave device is not already in this list you may type in its device address (a six-digit hex value) yourself.
Piconet Slave Address:
000406000006
< Back
Next >
Cancel
Help

Step 8 Select from the drop-down menu the hexadecimal address for your slave device into the box labeled **Piconet Slave Address**. If you do not see your slave's address, you can type it into the box.

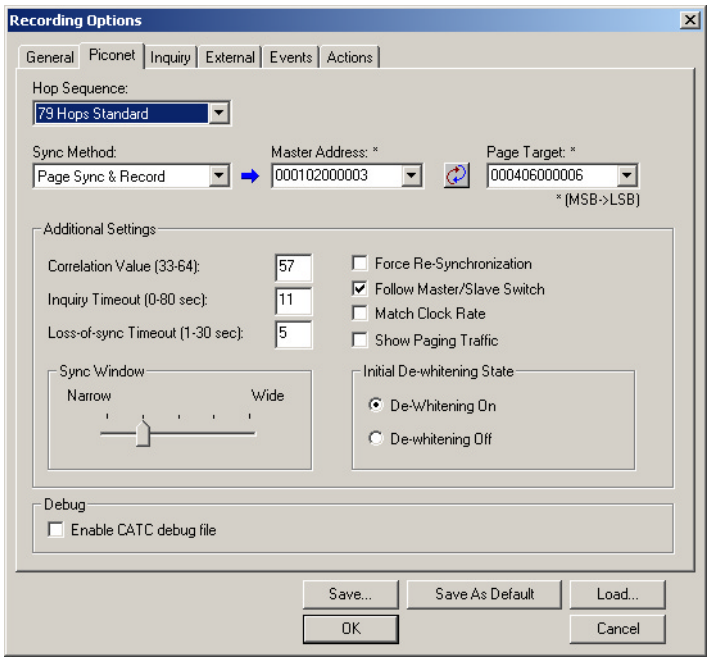
Step 9 Press **Next**.

The following screen will display.


Recording Wizard: New piconet (Step 8 of 8)
System is Ready
Initiate Search/Record
Merlin Mobile is now ready to synchronize to the piconet master when it attempts to page the pre-selected Slave device (using Merlin's Page Sync & Record mode). You will be prompted to establish the piconet only AFTER Merlin Mobile will enter the 'Synchronizing' state.
The following options will be used:
Synchronization Method: Page Sync & Record
Frequency Band: Standard (79-hop) mode
Master address: 000102000003
Slave address: 000406000006
Advanced...
Press 'Next' to initiate the recording or 'Back' to return to the previous page.
< Back
Next >
Cancel
Help

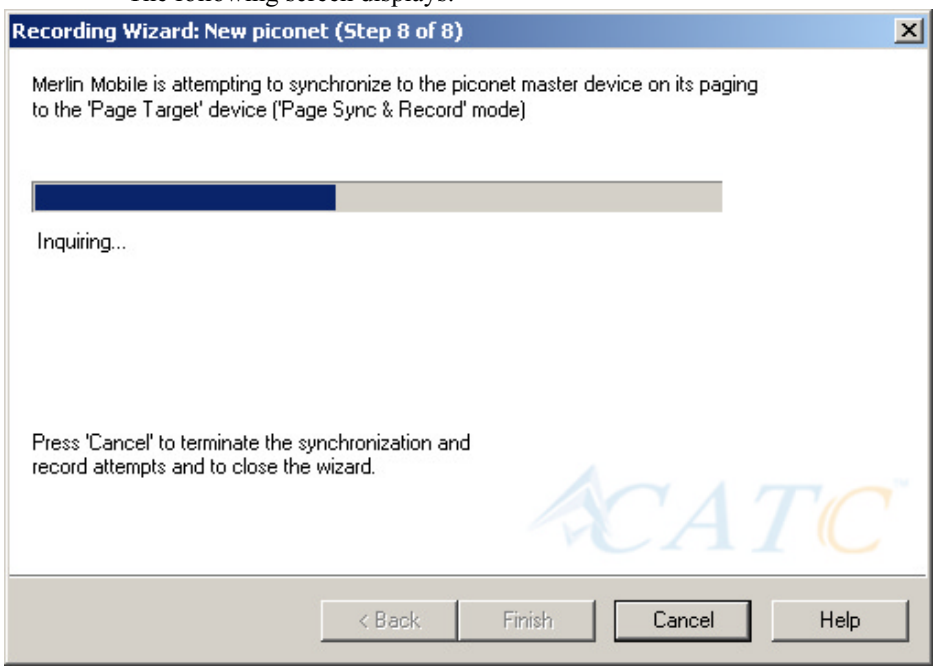
This screen displays the settings you selected.

The **Advanced** button on the right will open the Recording Options dialog box shown below. This screen will show the settings you selected through the Recording Wizard have been applied to the Recording Options dialog.



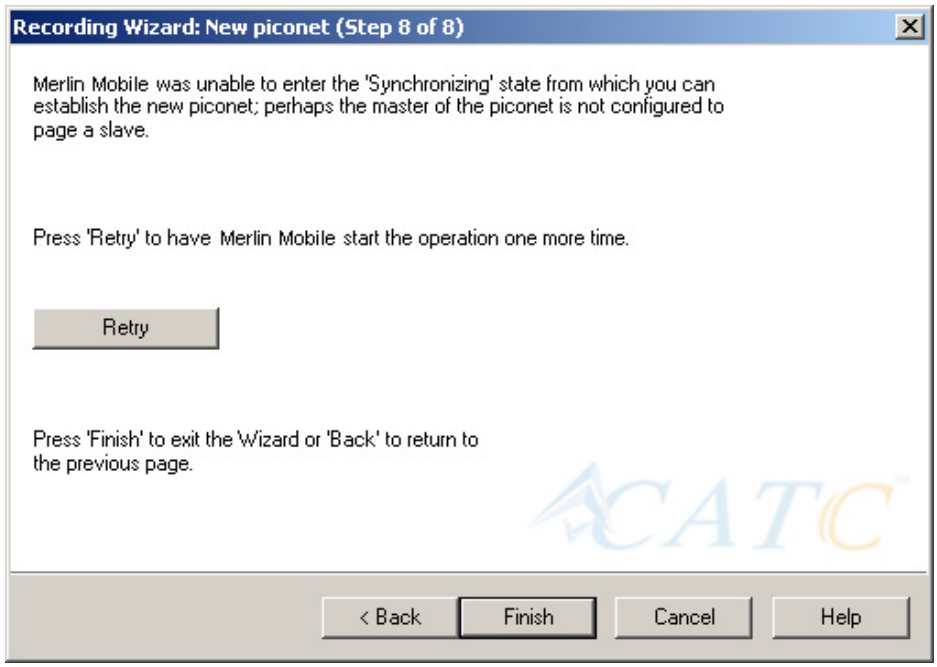
Step 10 Press **Next** to advance the Recording Wizard to the next screen.

The following screen displays:

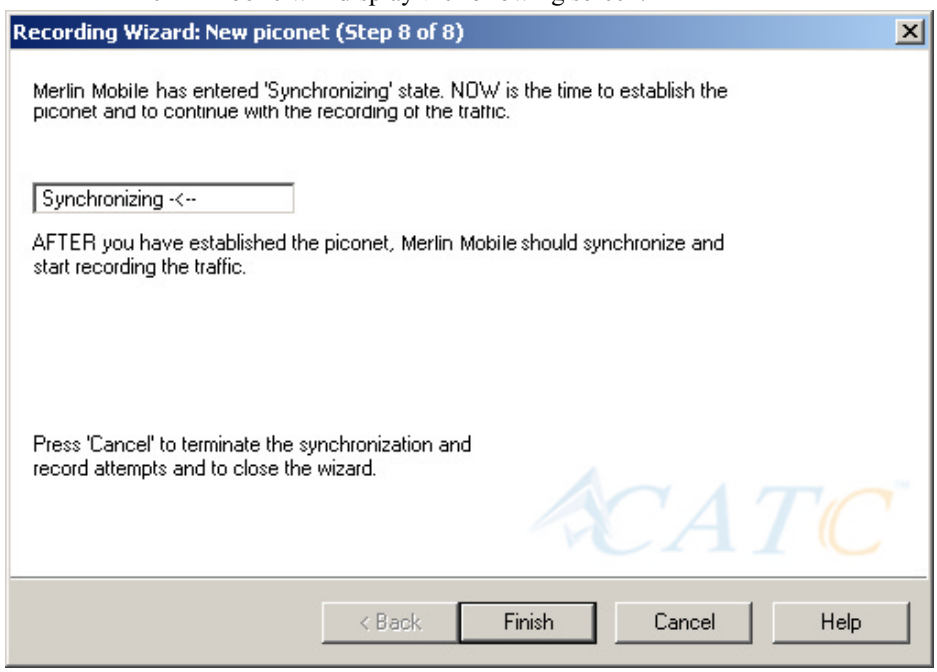

Recording Wizard: New piconet (Step 8 of 8)
Merlin Mobile is attempting to synchronize to the piconet master device on its paging to the 'Page Target' device ('Page Sync & Record' mode)
Inquiring...
Press 'Cancel' to terminate the synchronization and record attempts and to close the wizard.
< Back
Finish
Cancel
Help

Merlin Mobile pages the Master and if specified in Step 8, the Slave devices.

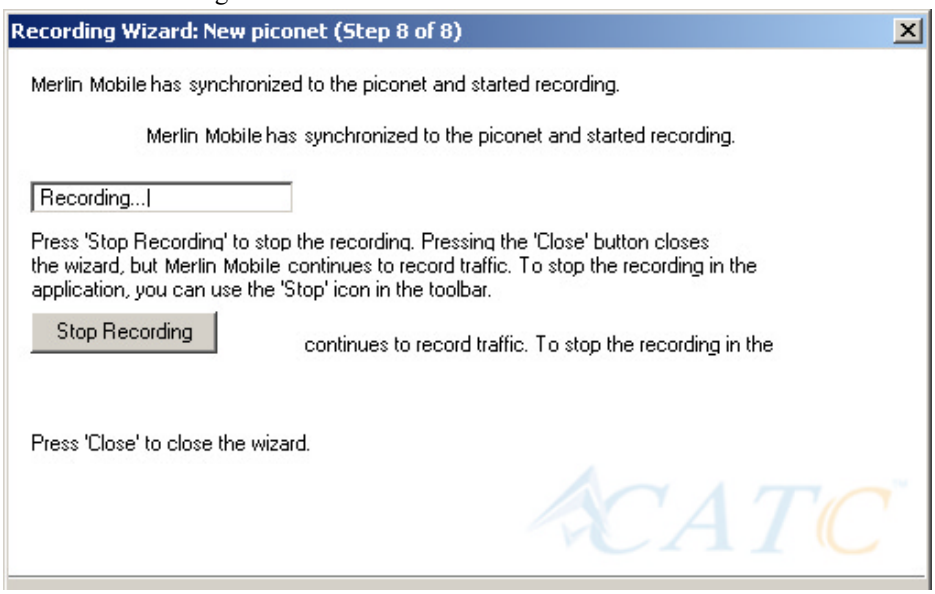
If Merlin Mobile is unable to complete its pages, the following screen will display:


Recording Wizard: New piconet (Step 8 of 8)
Merlin Mobile was unable to enter the 'Synchronizing' state from which you can establish the new piconet; perhaps the master of the piconet is not configured to page a slave.
Press 'Retry' to have Merlin Mobile start the operation one more time.
Retry
Press 'Finish' to exit the Wizard or 'Back' to return to the previous page.
< Back
Finish
Cancel
Help

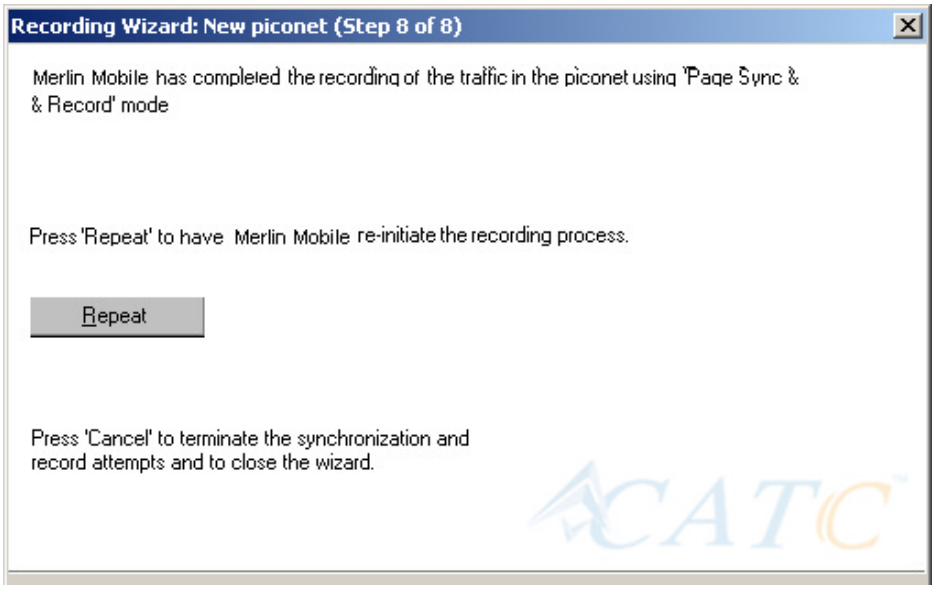
If Merlin Mobile is able to complete its pages, it will enter into a synchronizing state and then wait for you to create the piconet. During this waiting period, Merlin Mobile will display the following screen:


Recording Wizard: New piconet (Step 8 of 8)
Merlin Mobile has entered 'Synchronizing' state. NOW is the time to establish the piconet and to continue with the recording of the traffic.
Synchronizing -<--
AFTER you have established the piconet, Merlin Mobile should synchronize and start recording the traffic.
Press 'Cancel' to terminate the synchronization and record attempts and to close the wizard.
< Back
Finish
Cancel
Help

Once you have created the piconet, Merlin Mobile will synchronize to the piconet and begin recording. During the recording, Merlin Mobile will display the following screen:


Recording Wizard: New piconet (Step 8 of 8)
Merlin Mobile has synchronized to the piconet and started recording.
Merlin Mobile has synchronized to the piconet and started recording.
Recording...|
Press 'Stop Recording' to stop the recording. Pressing the 'Close' button closes the wizard, but Merlin Mobile continues to record traffic. To stop the recording in the application, you can use the 'Stop' icon in the toolbar.
Stop Recording
continues to record traffic. To stop the recording in the
Press 'Close' to close the wizard.

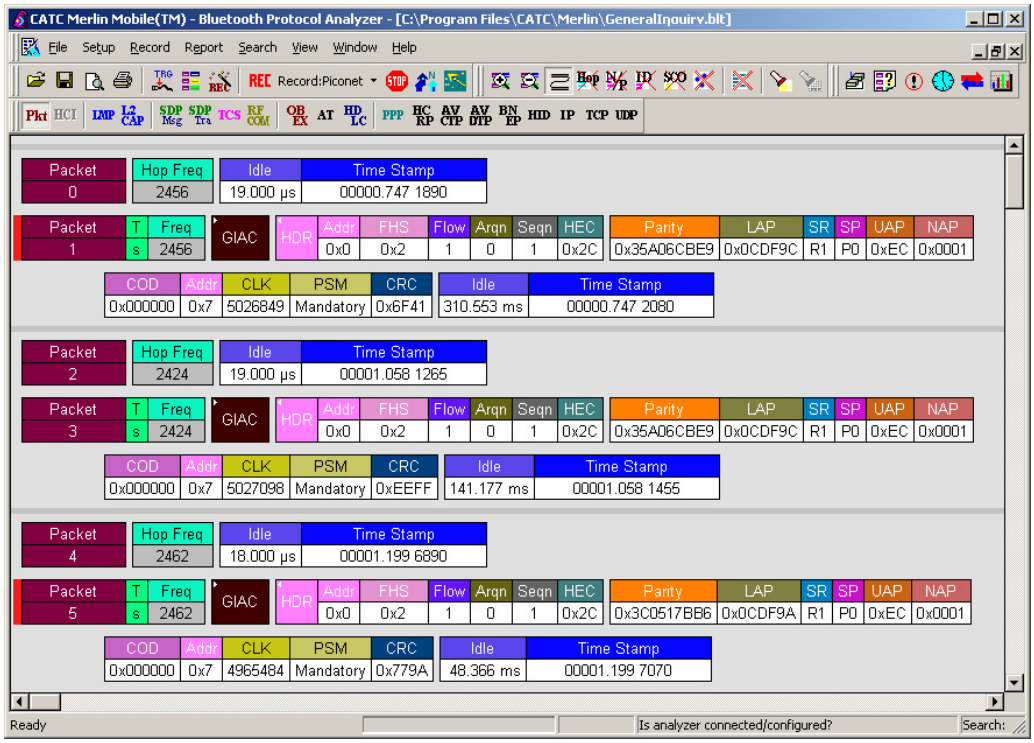
At the completion of the recording, Merlin Mobile will display the following screen:


Recording Wizard: New piconet (Step 8 of 8)
Merlin Mobile has completed the recording of the traffic in the piconet using 'Page Sync & & Record' mode
Press 'Repeat' to have Merlin Mobile re-initiate the recording process.
Repeat
Press 'Cancel' to terminate the synchronization and record attempts and to close the wizard.

You can repeat the recording by pressing the **Repeat** button.

Step 11 To close the wizard, press the **Close** button.

The wizard will close and your trace will display.

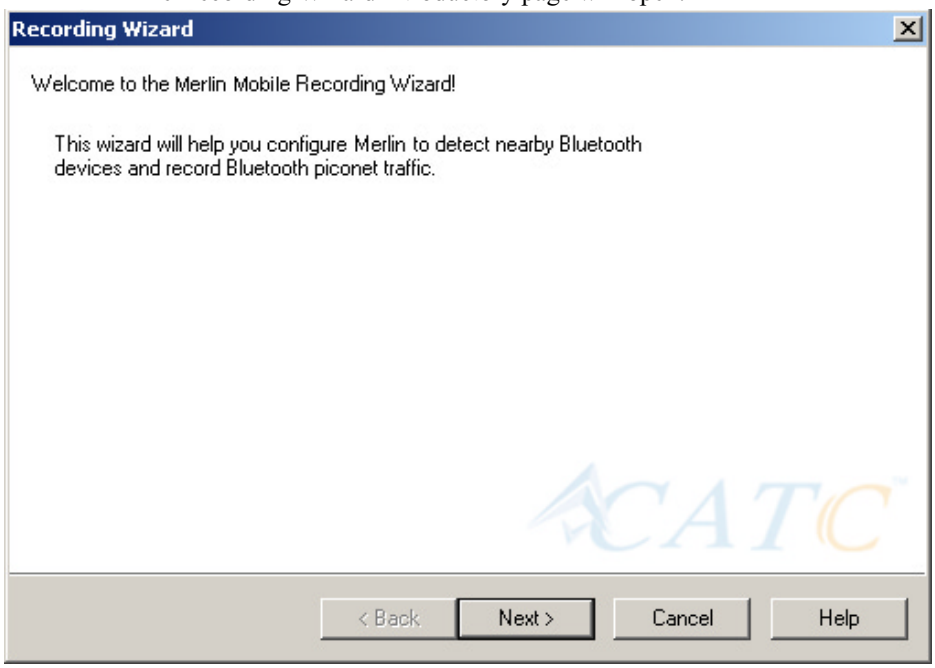

CATC Merlin Mobile(TM) - Bluetooth Protocol Analyzer - [C:\Program Files\CATC\Merlin\GeneralInquiry.blt]
File Setup Record Report Search View Window Help
REC Record:Piconet
Packet 0 | Hop Freq 2456 | Idle 19.000 µs | Time Stamp 00000.747 1890
Packet 1 | T s | Freq 2456 | GIAC | HDR | Addr 0x0 | FHS 0x2 | Flow 1 | Arqn 0 | Seqn 1 | HEC 0x2C | Parity 0x35A06CBE9 | LAP 0x0CDF9C | SR R1 | SP P0 | UAP 0xEC | NAP 0x0001
COD 0x000000 | Addr 0x7 | CLK 5026849 | PSM Mandatory | CRC 0x6F41 | Idle 310.553 ms | Time Stamp 00000.747 2080
Packet 2 | Hop Freq 2424 | Idle 19.000 µs | Time Stamp 00001.058 1265
Packet 3 | T s | Freq 2424 | GIAC | HDR | Addr 0x0 | FHS 0x2 | Flow 1 | Arqn 0 | Seqn 1 | HEC 0x2C | Parity 0x35A06CBE9 | LAP 0x0CDF9C | SR R1 | SP P0 | UAP 0xEC | NAP 0x0001
COD 0x000000 | Addr 0x7 | CLK 5027098 | PSM Mandatory | CRC 0xEEFF | Idle 141.177 ms | Time Stamp 00001.058 1455
Packet 4 | Hop Freq 2462 | Idle 18.000 µs | Time Stamp 00001.199 6890
Packet 5 | T s | Freq 2462 | GIAC | HDR | Addr 0x0 | FHS 0x2 | Flow 1 | Arqn 0 | Seqn 1 | HEC 0x2C | Parity 0x3C0517BB6 | LAP 0x0CDF9A | SR R1 | SP P0 | UAP 0xEC | NAP 0x0001
COD 0x000000 | Addr 0x7 | CLK 4965484 | PSM Mandatory | CRC 0x779A | Idle 48.366 ms | Time Stamp 00001.199 7070
Ready
Is analyzer connected/configured?
Search:

5.2 Recording an Existing Piconet

Using Recording Wizard to record an existing piconet is similar to recording a new piconet. The main difference is that you will be asked if your Master device can support multiple slave devices and whether it can respond to pages once it has created a piconet with another device.

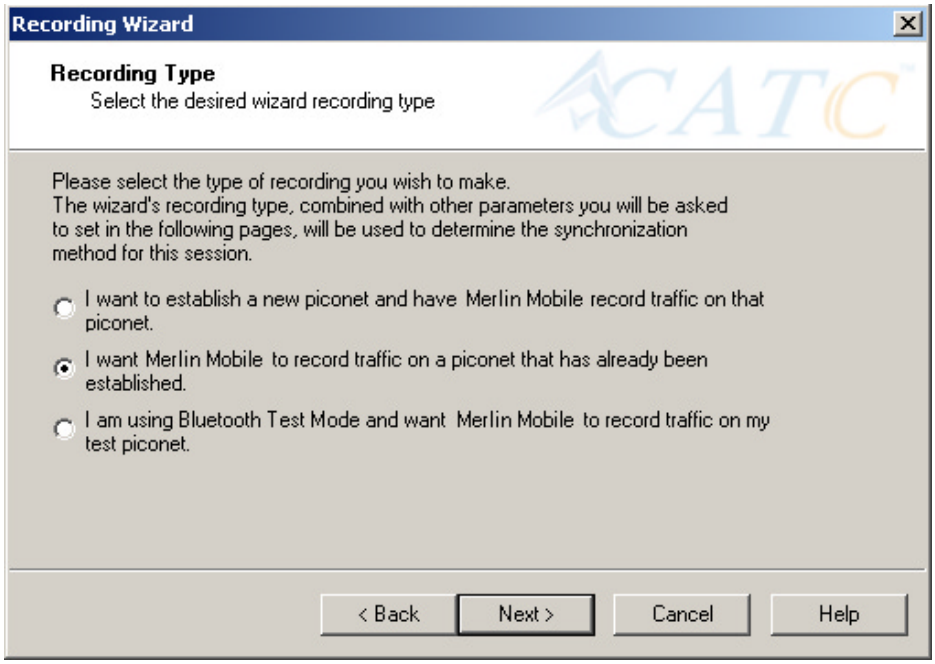
Step 1 To start the Recording Wizard, press or select **Setup > Recording Wizard** from the menu.

The Recording Wizard introductory page will open:


Recording Wizard
Welcome to the Merlin Mobile Recording Wizard!
This wizard will help you configure Merlin to detect nearby Bluetooth devices and record Bluetooth piconet traffic.
< Back
Next >
Cancel
Help

Step 2 Press **Next** to advance to the next screen.

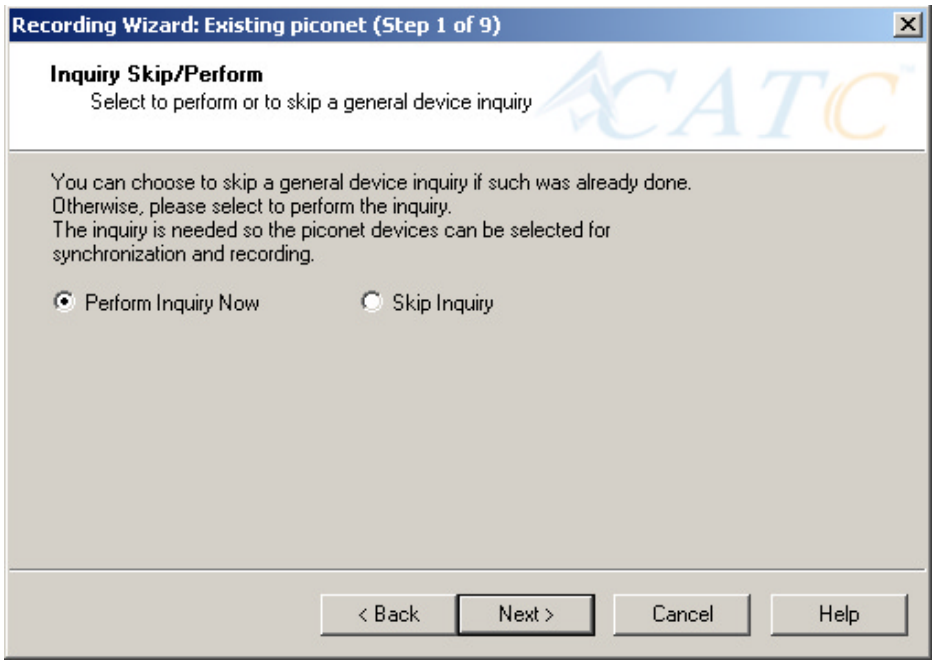
You will see three choices:


Recording Wizard
Recording Type
Select the desired wizard recording type
Please select the type of recording you wish to make.
The wizard's recording type, combined with other parameters you will be asked to set in the following pages, will be used to determine the synchronization method for this session.
I want to establish a new piconet and have Merlin Mobile record traffic on that piconet.
I want Merlin Mobile to record traffic on a piconet that has already been established.
I am using Bluetooth Test Mode and want Merlin Mobile to record traffic on my test piconet.
< Back
Next >
Cancel
Help

Step 3 Select the second option: **I want Merlin Mobile to record traffic on a piconet that has already been established**.

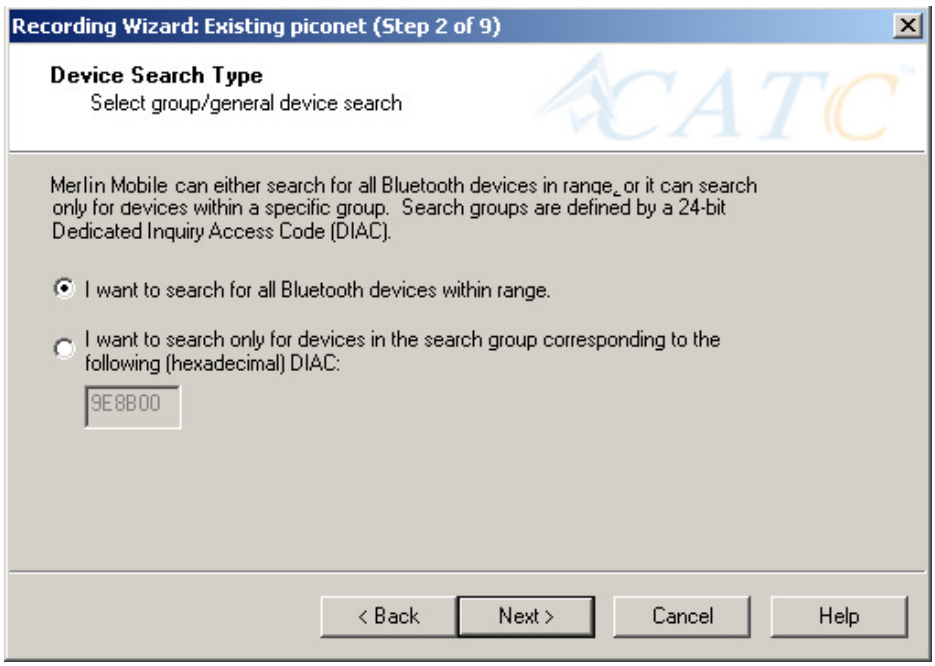
Step 4 Press **Next**.

You will see two choices:


Recording Wizard: Existing piconet (Step 1 of 9)
Inquiry Skip/Perform
Select to perform or to skip a general device inquiry
You can choose to skip a general device inquiry if such was already done.
Otherwise, please select to perform the inquiry.
The inquiry is needed so the piconet devices can be selected for
synchronization and recording.
Perform Inquiry Now
Skip Inquiry
< Back
Next >
Cancel
Help

Step 5 Select **Perform Inquiry Now**.

You will see two choices:

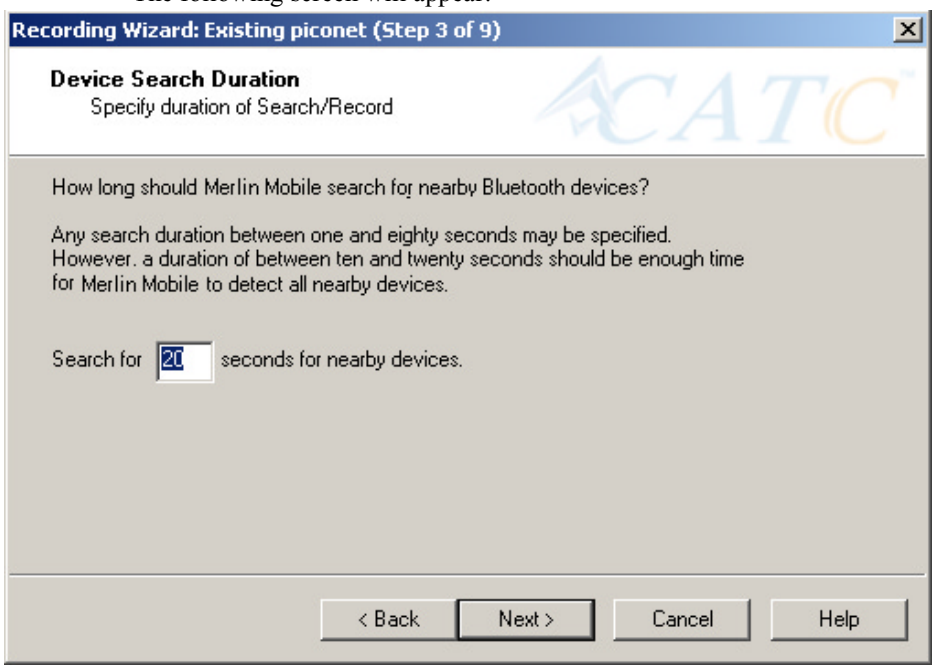

Recording Wizard: Existing piconet (Step 2 of 9)
Device Search Type
Select group/general device search
Merlin Mobile can either search for all Bluetooth devices in range, or it can search
only for devices within a specific group. Search groups are defined by a 24-bit
Dedicated Inquiry Access Code (DIAC).
I want to search for all Bluetooth devices within range.
I want to search only for devices in the search group corresponding to the
following (hexadecimal) DIAC:
9E8B00
< Back
Next >
Cancel
Help

Step 6 Select the first option: **I want Merlin Mobile to search for all Bluetooth devices within range**.

If you want to limit the inquiry to a class of devices, select the second option and enter the hexadecimal value for the device class in the text box.

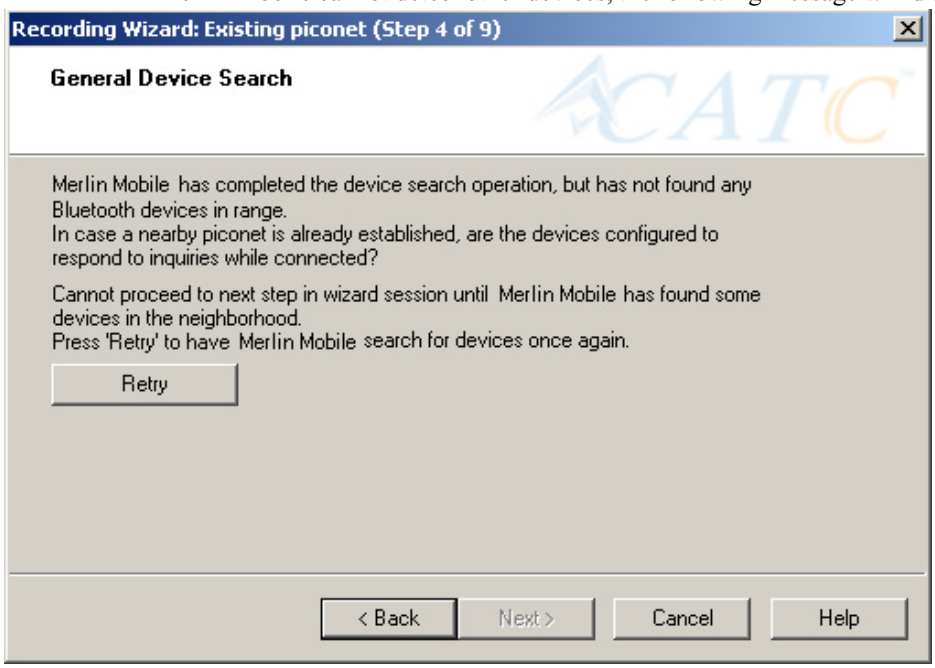
Step 7 Press **Next**.

The following screen will appear:

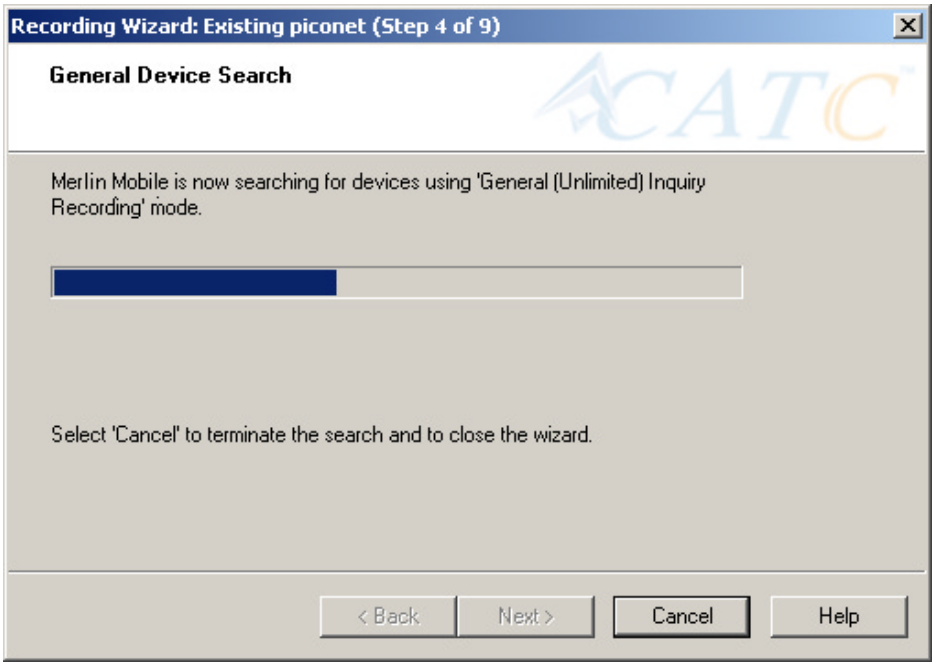

Recording Wizard: Existing piconet (Step 3 of 9)
Device Search Duration
Specify duration of Search/Record
How long should Merlin Mobile search for nearby Bluetooth devices?
Any search duration between one and eighty seconds may be specified.
However. a duration of between ten and twenty seconds should be enough time
for Merlin Mobile to detect all nearby devices.
Search for 20 seconds for nearby devices.
< Back
Next >
Cancel
Help

Step 8 If you want to change the search duration, type in a new value into the text box. Otherwise, use the default value (20 seconds), then press **Next**.

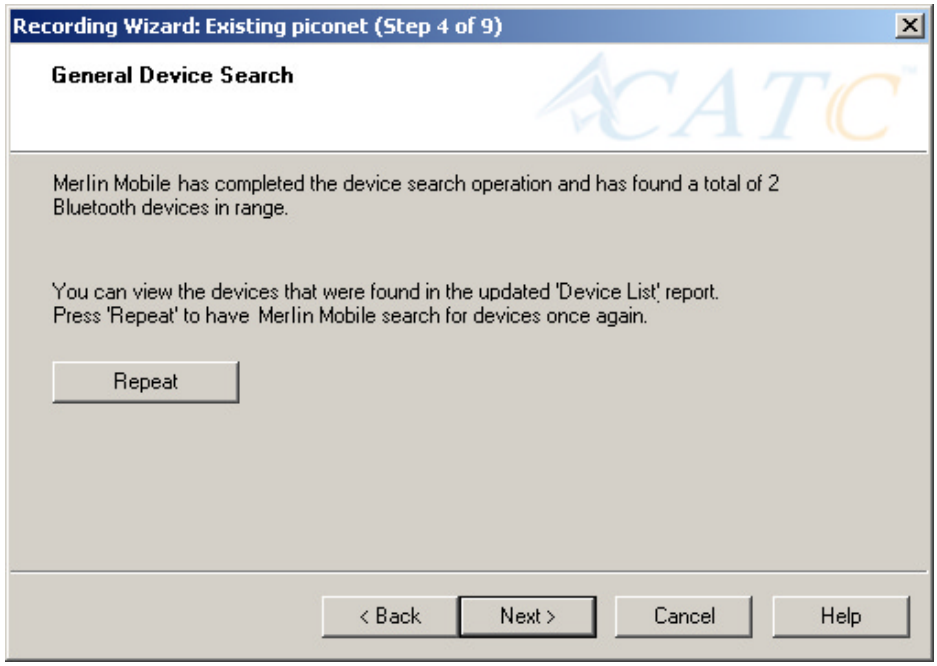
If Merlin Mobile cannot detect other devices, the following message will display:


Recording Wizard: Existing piconet (Step 4 of 9)
General Device Search
Merlin Mobile has completed the device search operation, but has not found any Bluetooth devices in range.
In case a nearby piconet is already established, are the devices configured to respond to inquiries while connected?
Cannot proceed to next step in wizard session until Merlin Mobile has found some devices in the neighborhood.
Press 'Retry' to have Merlin Mobile search for devices once again.
Retry
< Back
Next >
Cancel
Help

If Merlin Mobile passes the hardware test, it will then goes onto conduct a General Inquiry to locate local Bluetooth devices.


Recording Wizard: Existing piconet (Step 4 of 9)
General Device Search
Merlin Mobile is now searching for devices using 'General (Unlimited) Inquiry Recording' mode.
Select 'Cancel' to terminate the search and to close the wizard.
< Back
Next >
Cancel
Help

If Merlin Mobile finds Bluetooth devices, it will display the following message:


Recording Wizard: Existing piconet (Step 4 of 9)
General Device Search
Merlin Mobile has completed the device search operation and has found a total of 2 Bluetooth devices in range.
You can view the devices that were found in the updated 'Device List' report.
Press 'Repeat' to have Merlin Mobile search for devices once again.
Repeat
< Back
Next >
Cancel
Help

Check the Device List to see if Merlin Mobile found all of the devices in your piconet. If you feel that the list is incomplete, you can close this window and press the button marked **Repeat**. This will cause Merlin Mobile to repeat the General Inquiry and recollect information on local Bluetooth devices.

Step 9 Press **Next** to advance to the next screen.

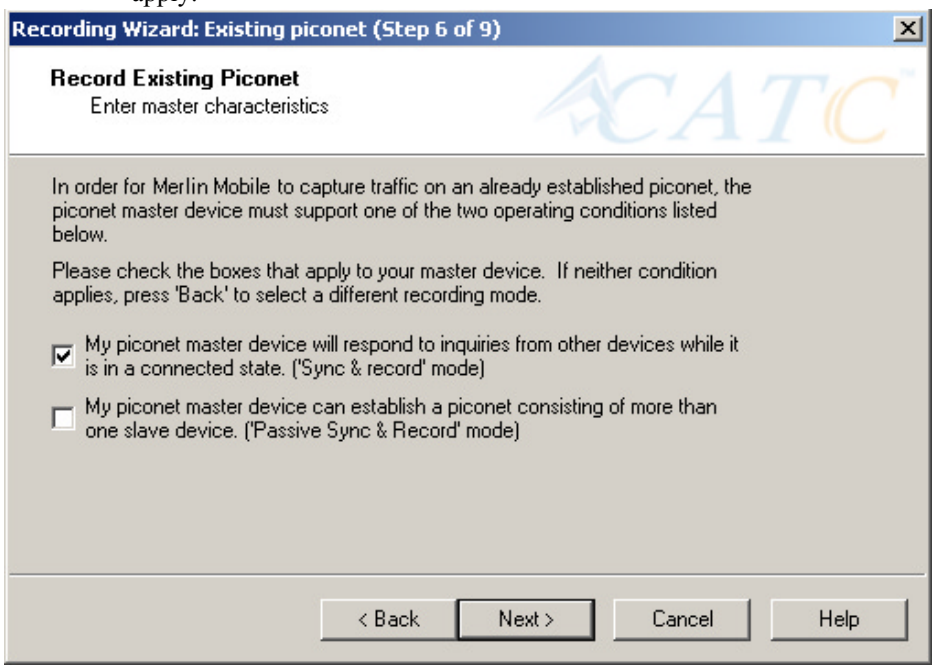
The following screen will prompt you for the Master device's address. The address can be selected from the menu or typed into the box:

Recording Wizard: Existing piconet - Specify Master Device (Step 5 of 9)
Device Address
Please select the Bluetooth device address of the master device for the piconet to be recorded.
The list below includes devices that Merlin Mobile has recently encountered. If your master device is not already in this list you may type in its device address (a six-digit hex value) yourself.
Piconet Master Address:
000281640DBA
< Back
Next >
Cancel
Help

Step 10 Select or type in the Master device's address into the box next to the label **Piconet Master Address**.

Step 11 Press **Next**.

The following screen will display. This screen asks you which of the following two options apply to your Master device. For some devices, both options will apply.


Recording Wizard: Existing piconet (Step 6 of 9)
Record Existing Piconet
Enter master characteristics
In order for Merlin Mobile to capture traffic on an already established piconet, the piconet master device must support one of the two operating conditions listed below.
Please check the boxes that apply to your master device. If neither condition applies, press 'Back' to select a different recording mode.
My piconet master device will respond to inquiries from other devices while it is in a connected state. ('Sync & record' mode)
My piconet master device can establish a piconet consisting of more than one slave device. ('Passive Sync & Record' mode)
< Back
Next >
Cancel
Help

You can select either or both options. They are not mutually exclusive:

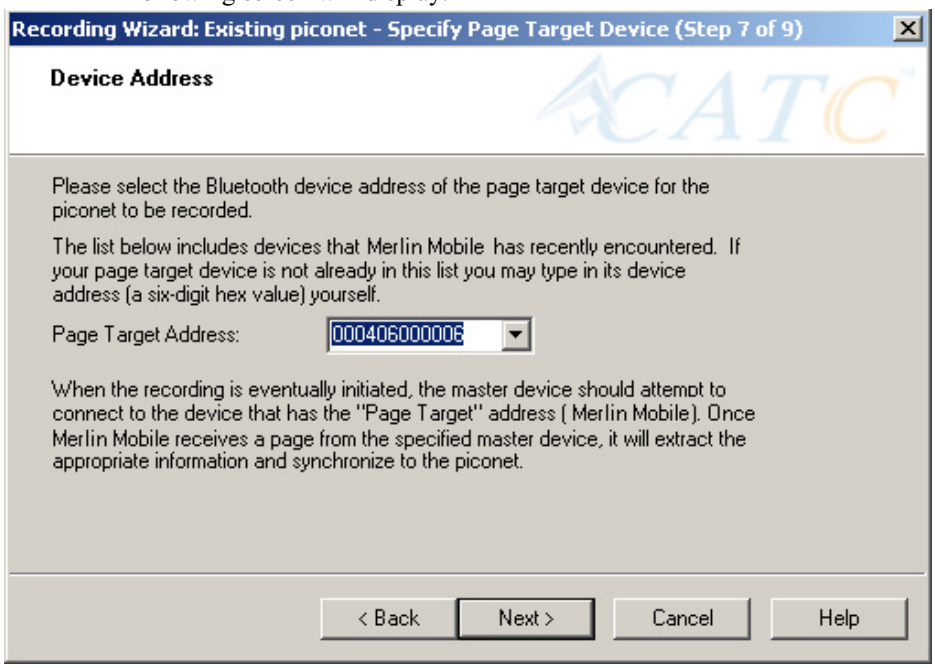
If the Master supports inquiries while in a connected state, select the first option. This will set Merlin Mobile to use the 'Sync & Record' mode in its attempts to synchronize to the Master. This will also cause the wizard to skip to step 8.

If the Master can support piconets with multiple slaves, select the second option. If you select this box alone (i.e., you leave the first box unchecked), Merlin Mobile will use the 'Passive Sync & Record' mode to synchronize to the Master. The wizard will then advance to Screen 8*.

If the first checkbox was selected, Merlin Mobile will use 'Sync & Record' no matter what was set in the second box.

Step 12 If you want to skip the Master verification, put a check in the box. If you are in doubt, leave the box unchecked.

If you selected only the second option in Step 12 (='Passive Sync & Record'), the following screen will display.


Recording Wizard: Existing piconet - Specify Page Target Device (Step 7 of 9)
Device Address
Please select the Bluetooth device address of the page target device for the piconet to be recorded.
The list below includes devices that Merlin Mobile has recently encountered. If your page target device is not already in this list you may type in its device address (a six-digit hex value) yourself.
Page Target Address:
000406000006
When the recording is eventually initiated, the master device should attempt to connect to the device that has the "Page Target" address (Merlin Mobile). Once Merlin Mobile receives a page from the specified master device, it will extract the appropriate information and synchronize to the piconet.
< Back
Next >
Cancel
Help

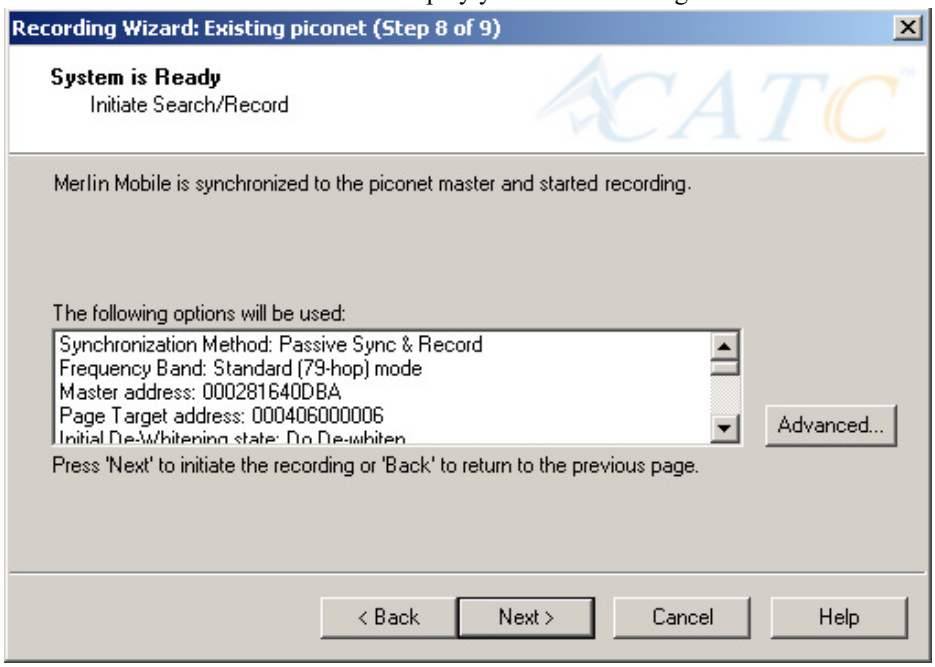
This screen asks you for the address of the Page Target device -- which in this case is Merlin Mobile. Since the devices in your piconet are not able to respond to inquiries, Merlin Mobile will not be able to page the devices and join the piconet. Instead, you will assign Merlin Mobile an address here in this screen, then direct your piconet Master device to connect to Merlin Mobile. The Master will attempt to connect to Merlin Mobile and therein give Merlin Mobile the information it needs to record the Master and slave devices.

Step 13 Type in an address of your choosing for Merlin Mobile (= Page Target).

You are making up an address for Merlin Mobile that the Master will use to try to connect to Merlin Mobile.

Step 14 Press **Next**

Merlin Mobile will then display your current settings.


Recording Wizard: Existing piconet (Step 8 of 9)
System is Ready
Initiate Search/Record
Merlin Mobile is synchronized to the piconet master and started recording.
The following options will be used:
Synchronization Method: Passive Sync & Record
Frequency Band: Standard (79-hop) mode
Master address: 000281640DBA
Page Target address: 000406000006
Advanced...
Press 'Next' to initiate the recording or 'Back' to return to the previous page.
< Back
Next >
Cancel
Help

The **Advanced** button will open the Recording Options dialog box shown on page 41 and described in detail in Chapter 7.

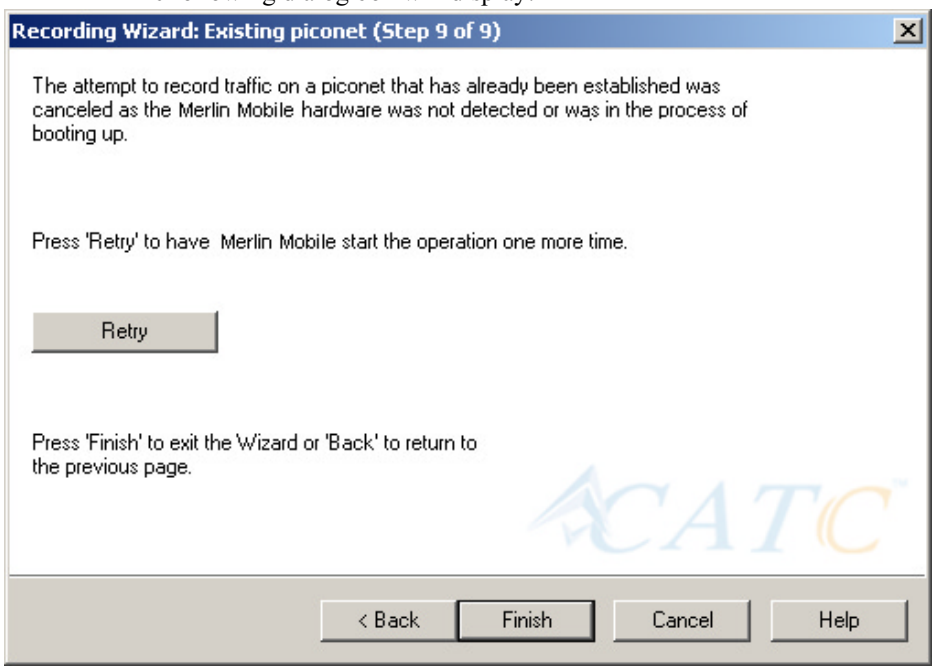
Step 15 Press **Next** to begin the recording.

If the Merlin Mobile hardware is not ready or connected or is in the process of booting up, the following information message box will display:

BTTracer
Your Merlin Mobile was not detected; it may not be connected properly to this computer or may not be powered on.
Please verify that your Merlin Mobile is connected with a USB cable to this computer, that the Merlin Mobile power LED is on, and that the trigger LED is not flashing.
If the trigger LED is flashing, this indicates a hardware problem; please contact your distributor for service.
If you have found the source of the problem, press 'OK' to close this message-box, and then press 'Retry' in the Wizard to retry the operation or press 'Cancel' to exit the Recording Wizard.
OK

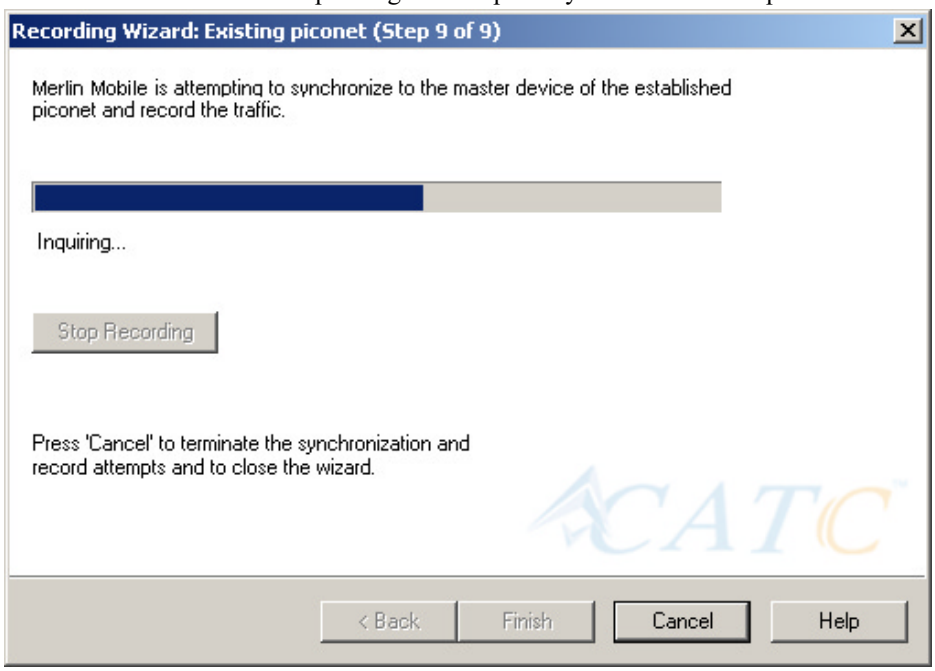
Step 16 If the above information box opened, press **OK** to close it.

The following dialog box will display:


Recording Wizard: Existing piconet (Step 9 of 9)
The attempt to record traffic on a piconet that has already been established was canceled as the Merlin Mobile hardware was not detected or was in the process of booting up.
Press 'Retry' to have Merlin Mobile start the operation one more time.
Retry
Press 'Finish' to exit the Wizard or 'Back' to return to the previous page.
< Back
Finish
Cancel
Help

Step 17 Press **Retry** or **Back** to re-attempt the process.

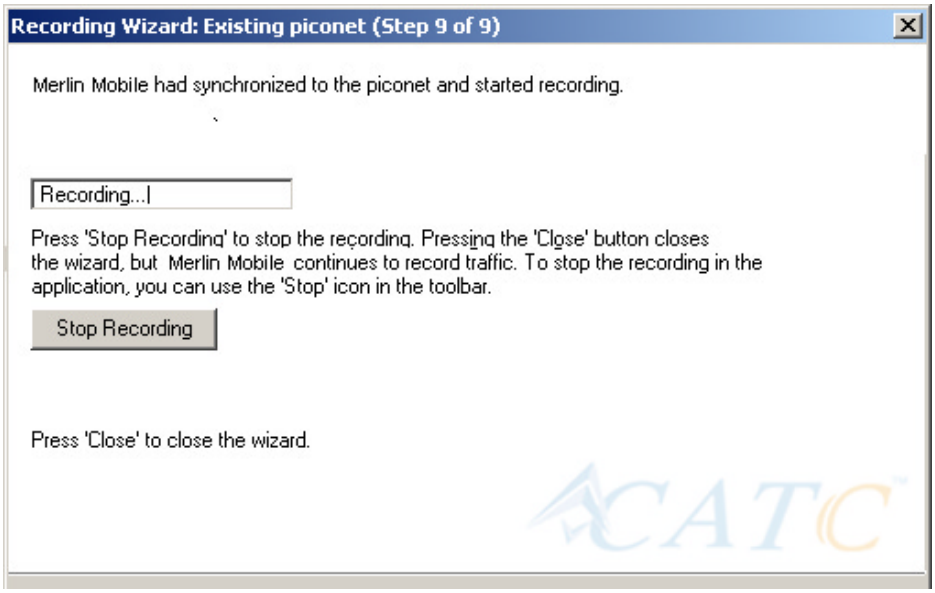
If the hardware failure described above do not occur, Merlin Mobile will conduct an inquiry. The screen will show that Merlin Mobile is going to attempt a recording in either 'Passive Sync & Record' mode as shown below or in 'Sync & Record' mode depending on the options you selected in Step 15.


Recording Wizard: Existing piconet (Step 9 of 9)
Merlin Mobile is attempting to synchronize to the master device of the established piconet and record the traffic.
Inquiring...
Stop Recording
Press 'Cancel' to terminate the synchronization and record attempts and to close the wizard.
< Back
Finish
Cancel
Help

Step 18 If you are recording in 'Passive Sync & Record' mode, you will

need to direct your Master device to attempt a connection to Merlin Mobile. This will provide Merlin Mobile with the information it needs to record the piconet.

Once Merlin Mobile has the information it needs, it will begin recording. The following screen will display:


Recording Wizard: Existing piconet (Step 9 of 9)
Merlin Mobile had synchronized to the piconet and started recording.
Recording...
Press 'Stop Recording' to stop the recording. Pressing the 'Close' button closes the wizard, but Merlin Mobile continues to record traffic. To stop the recording in the application, you can use the 'Stop' icon in the toolbar.
Stop Recording
Press 'Close' to close the wizard.

The recording will end following a trigger event or when you press **Stop Recording** button on the screen shown above or when you press the button on the toolbar.

Step 19 When finished, press **Close** to close the Recording Wizard.

5.3 Recording in Test Mode

A Test Mode recording allows you to limit the frequency hopping range that Merlin Mobile will record. Two Test Modes are available: Reduced Hopping Mode and Single Frequency Mode. Reduced Hopping Mode limits Merlin Mobile's recording to the five frequency hops that are described in the Bluetooth Specification. Single Frequency Mode limits Merlin Mobile's recording to a single frequency range that you specify in the Recording Wizard.

Recording in Reduced Hopping Mode

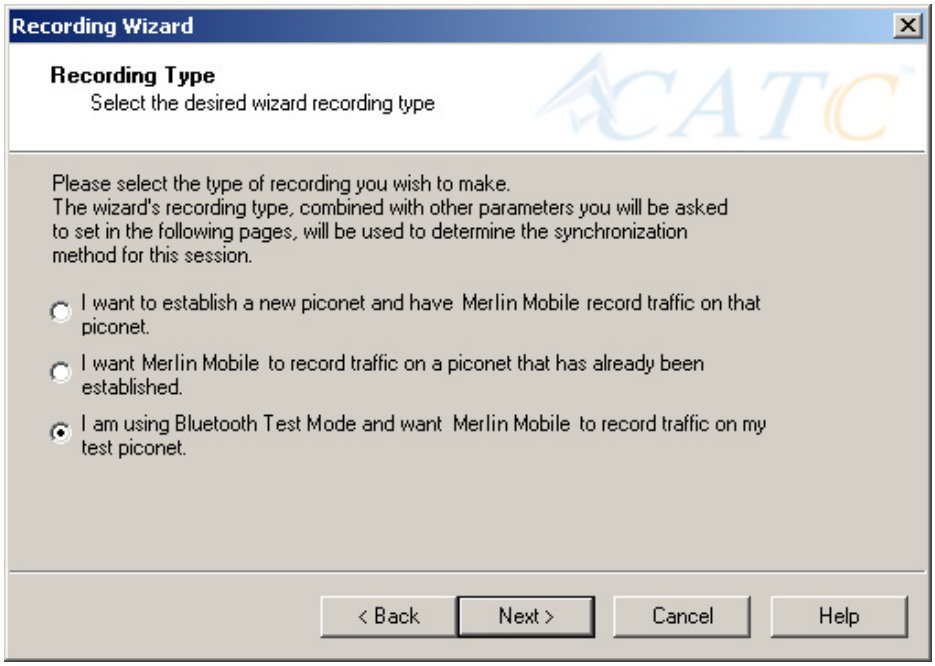
To record in Reduced Hopping Mode, perform the following steps:

Step 1 Start the Recording Wizard by either pressing the button or selecting **Setup > Recording Wizard** from the menu.

The Recording Wizard greeting screen will open.

Step 2 Press **Next** to advance to the **Recording Type** screen.

The following screen will display:

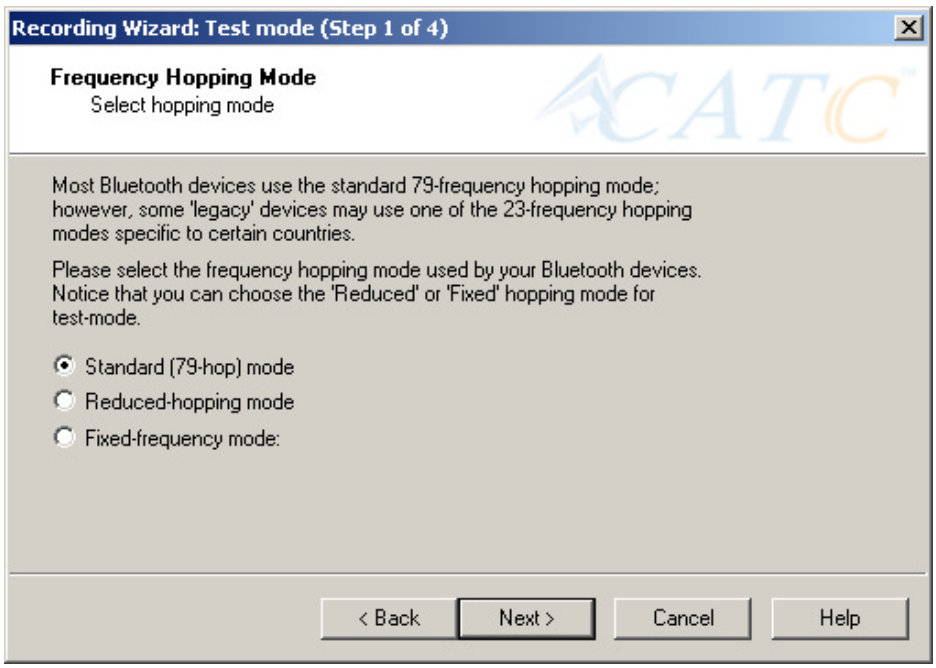

Recording Wizard
Recording Type
Select the desired wizard recording type
Please select the type of recording you wish to make.
The wizard's recording type, combined with other parameters you will be asked to set in the following pages, will be used to determine the synchronization method for this session.
I want to establish a new piconet and have Merlin Mobile record traffic on that piconet.
I want Merlin Mobile to record traffic on a piconet that has already been established.
I am using Bluetooth Test Mode and want Merlin Mobile to record traffic on my test piconet.
< Back
Next >
Cancel
Help

Step 3 Select the third option: **I am using Bluetooth Test Mode and want Merlin Mobile to record traffic on my test**

piconet.

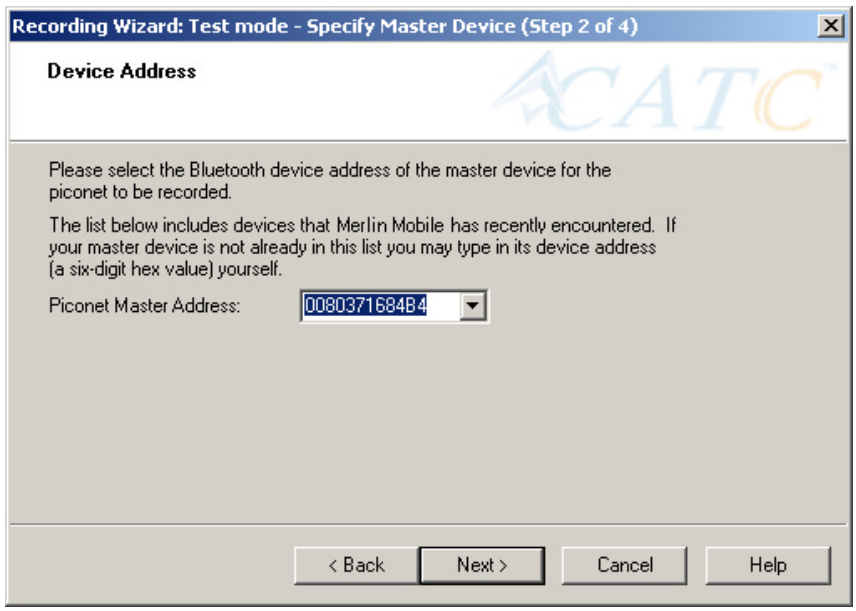
Step 4 Press **Next**.

The following screen will display:


Recording Wizard: Test mode (Step 1 of 4)
Frequency Hopping Mode
Select hopping mode
Most Bluetooth devices use the standard 79-frequency hopping mode; however, some 'legacy' devices may use one of the 23-frequency hopping modes specific to certain countries.
Please select the frequency hopping mode used by your Bluetooth devices. Notice that you can choose the 'Reduced' or 'Fixed' hopping mode for test-mode.
Standard (79-hop) mode
Reduced-hopping mode
Fixed-frequency mode:
< Back
Next >
Cancel
Help

Step 5 Select the option **Reduced-hopping mode**, then press **Next**.

The following screen will display:

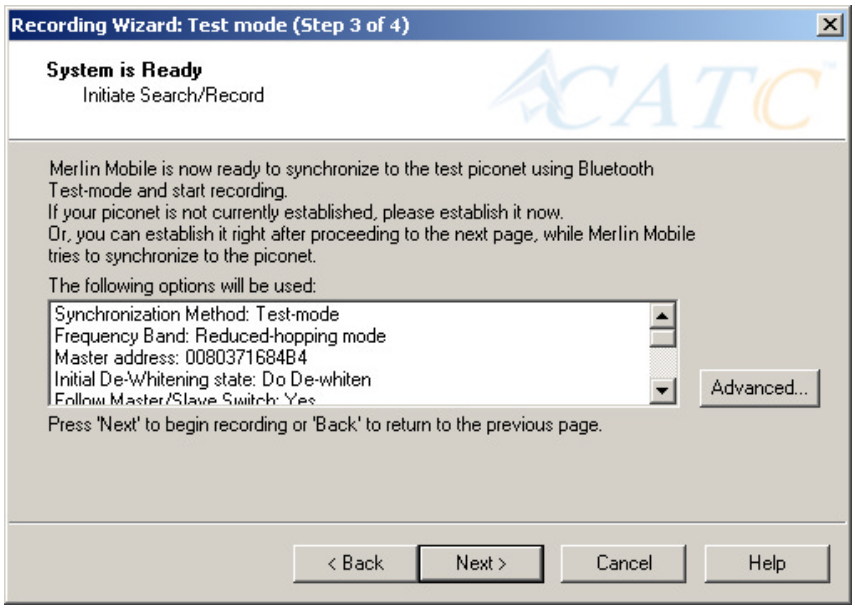

Recording Wizard: Test mode - Specify Master Device (Step 2 of 4)
Device Address
Please select the Bluetooth device address of the master device for the piconet to be recorded.
The list below includes devices that Merlin Mobile has recently encountered. If your master device is not already in this list you may type in its device address (a six-digit hex value) yourself.
Piconet Master Address:
00803716B4B4
< Back
Next >
Cancel
Help

Step 6 Select the address for your piconet's Master device from the drop-down menu. If you prefer, you can type in the address

into the box.

Step 7 Press **Next**.

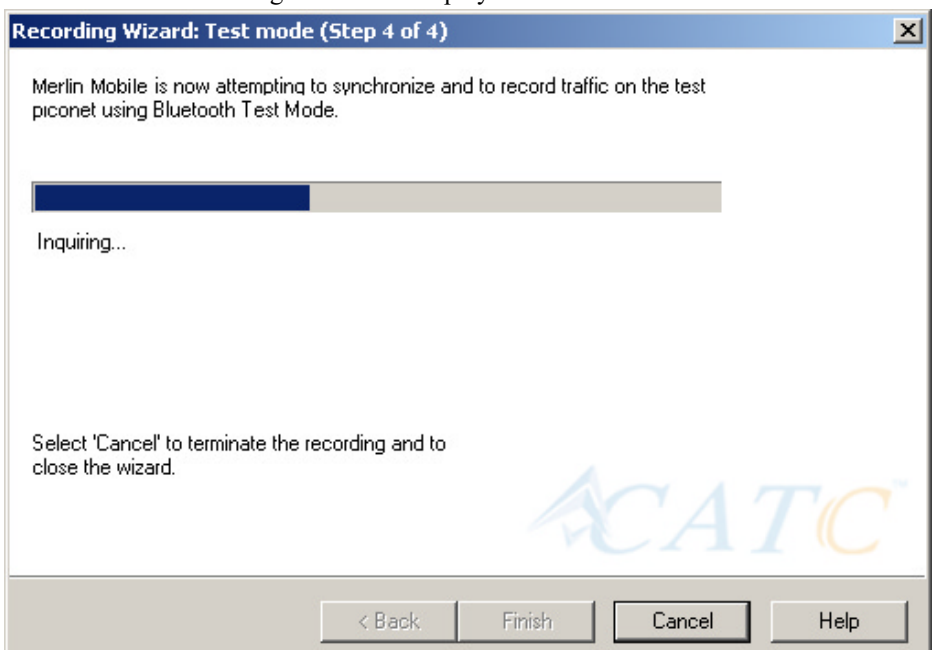
The following screen will display. This screen will show the current settings for the recording:


Recording Wizard: Test mode (Step 3 of 4)
System is Ready
Initiate Search/Record
Merlin Mobile is now ready to synchronize to the test piconet using Bluetooth Test-mode and start recording.
If your piconet is not currently established, please establish it now.
Or, you can establish it right after proceeding to the next page, while Merlin Mobile tries to synchronize to the piconet.
The following options will be used:
Synchronization Method: Test-mode
Frequency Band: Reduced-hopping mode
Master address: 0080371684B4
Initial De-Whitening state: Do De-whiten
Advanced...
Press 'Next' to begin recording or 'Back' to return to the previous page.
< Back
Next >
Cancel
Help

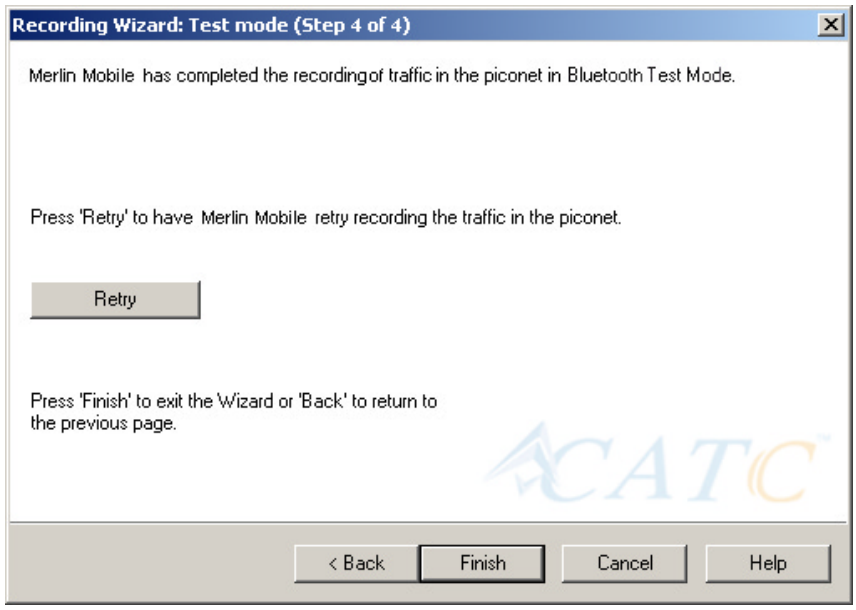
The Advanced button will open the Recording Options dialog box. See Chapter 7 for details on the Recording Options dialog box.

Step 8 Press **Next** to begin the recording.

The following screen will display:


Recording Wizard: Test mode (Step 4 of 4)
Merlin Mobile is now attempting to synchronize and to record traffic on the test piconet using Bluetooth Test Mode.
Inquiring...
Select 'Cancel' to terminate the recording and to close the wizard.
< Back
Finish
Cancel
Help

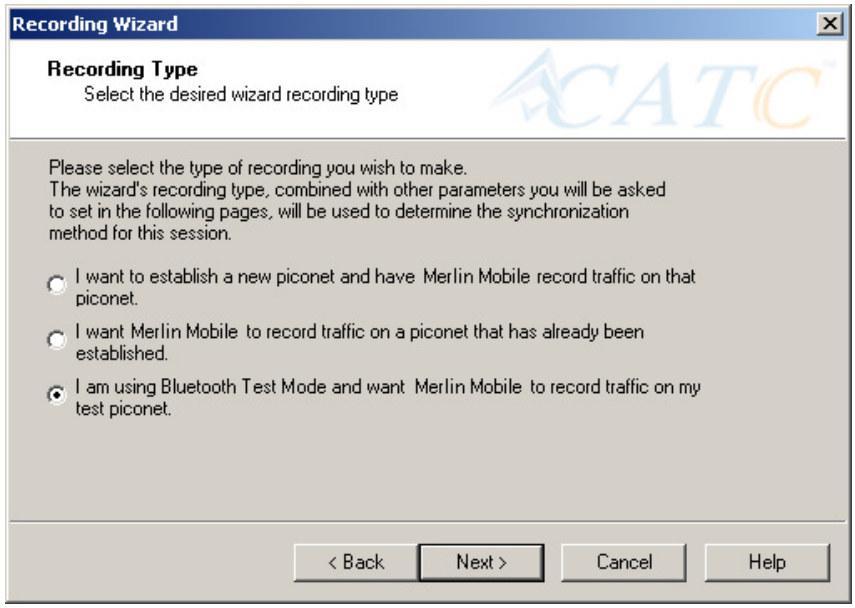
Step 9 When the recording finishes, the following screen will display. You can repeat the recording by pressing the **Repeat** button.


Recording Wizard: Test mode (Step 4 of 4)
Merlin Mobile has completed the recording of traffic in the piconet in Bluetooth Test Mode.
Press 'Retry' to have Merlin Mobile retry recording the traffic in the piconet.
Retry
Press 'Finish' to exit the Wizard or 'Back' to return to the previous page.
< Back
Finish
Cancel
Help

Step 10 To close the wizard, press **Finish**.

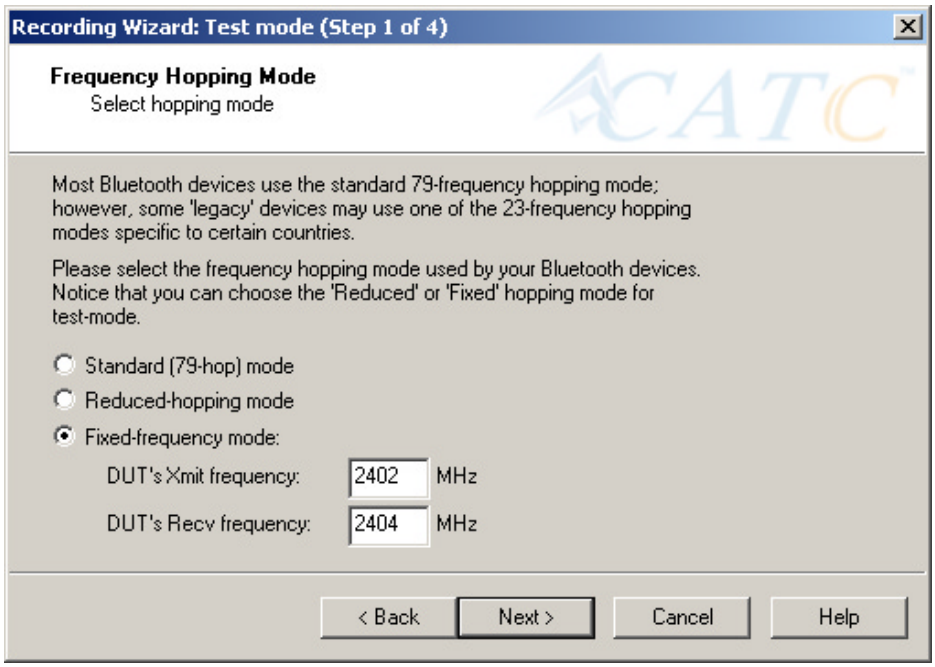
5.4 Recording in Single Frequency Mode

Step 1 In the Recording Type window, select the third radio button


Recording Wizard
Recording Type
Select the desired wizard recording type
Please select the type of recording you wish to make.
The wizard's recording type, combined with other parameters you will be asked to set in the following pages, will be used to determine the synchronization method for this session.
I want to establish a new piconet and have Merlin Mobile record traffic on that piconet.
I want Merlin Mobile to record traffic on a piconet that has already been established.
I am using Bluetooth Test Mode and want Merlin Mobile to record traffic on my test piconet.
< Back
Next >
Cancel
Help

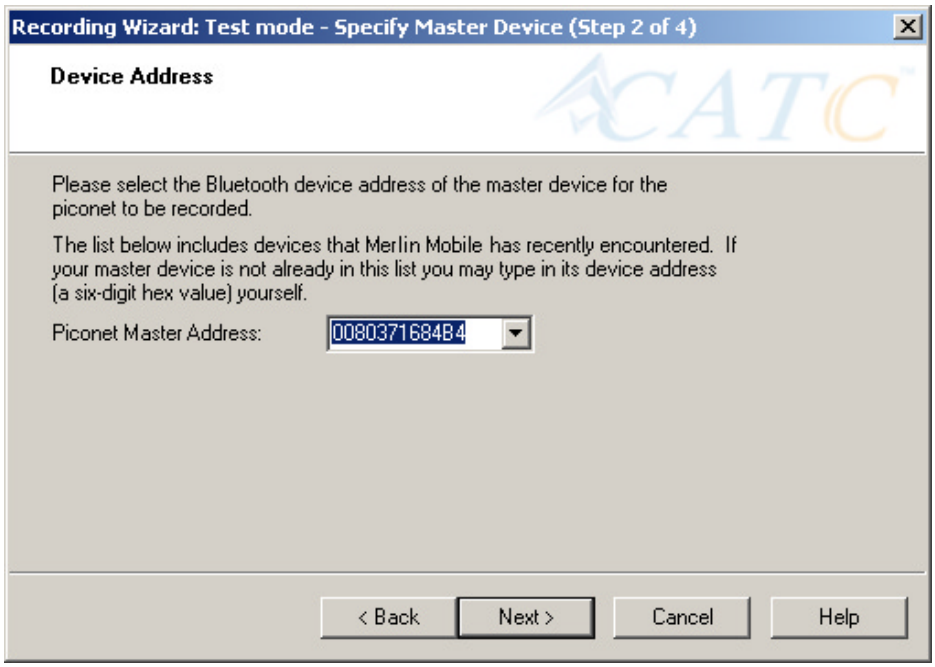
and click **Next**.

Step 2 In the **Frequency Hopping Mode**, window select the **Fixed-Frequency Mode** radio button, enter the appropriate values in the text boxes, and click **Next**.

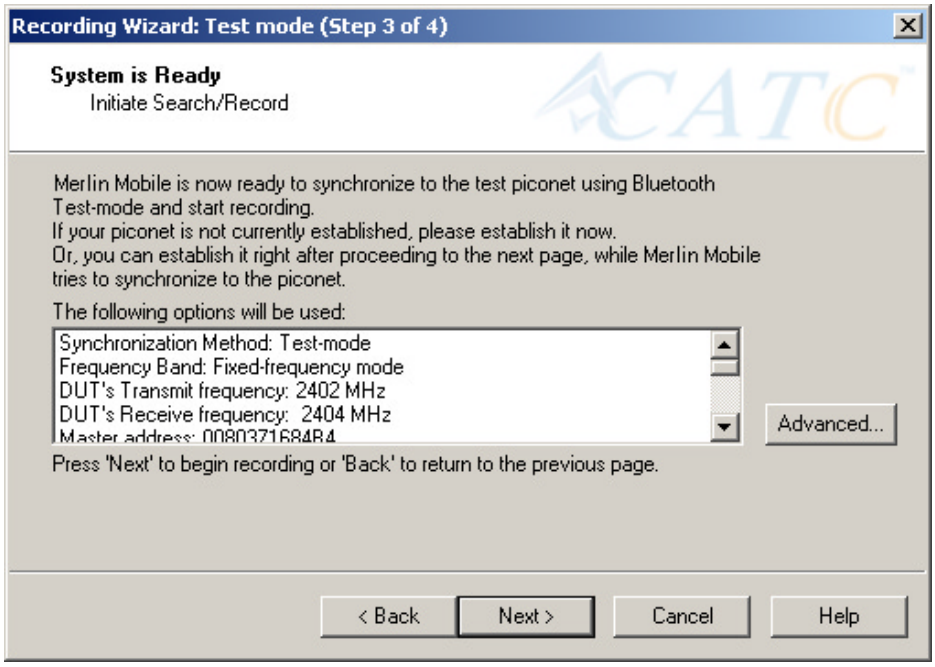

Recording Wizard: Test mode (Step 1 of 4)
Frequency Hopping Mode
Select hopping mode
Most Bluetooth devices use the standard 79-frequency hopping mode; however, some 'legacy' devices may use one of the 23-frequency hopping modes specific to certain countries.
Please select the frequency hopping mode used by your Bluetooth devices. Notice that you can choose the 'Reduced' or 'Fixed' hopping mode for test-mode.
Standard (79-hop) mode
Reduced-hopping mode
Fixed-frequency mode:
DUT's Xmit frequency: 2402 MHz
DUT's Recv frequency: 2404 MHz
< Back
Next >
Cancel
Help

Step 3 In the Master Device address box, enter the BD Address for

your Master Device.

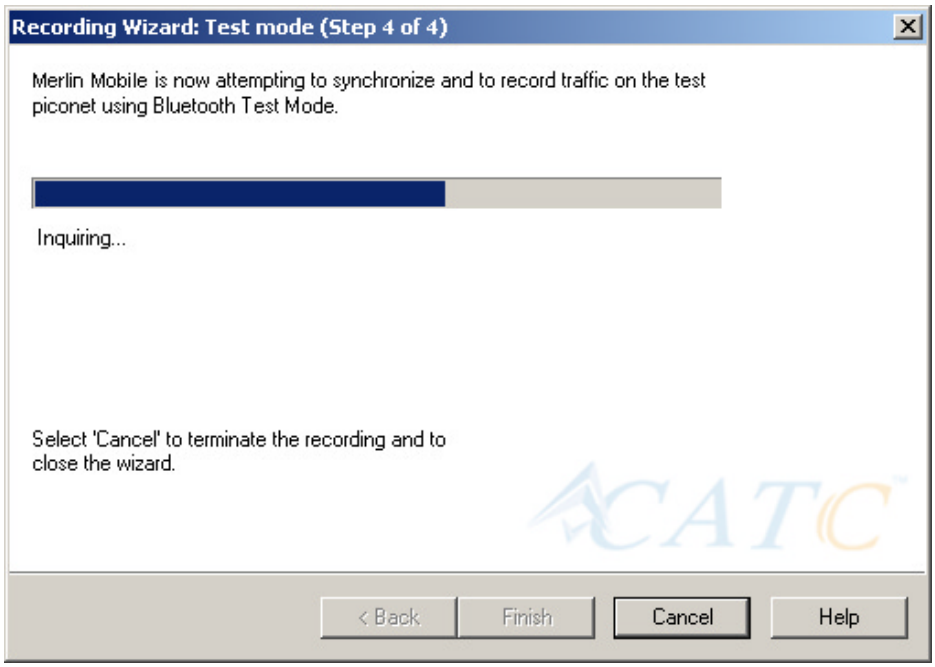

Recording Wizard: Test mode - Specify Master Device (Step 2 of 4)
Device Address
Please select the Bluetooth device address of the master device for the piconet to be recorded.
The list below includes devices that Merlin Mobile has recently encountered. If your master device is not already in this list you may type in its device address (a six-digit hex value) yourself.
Piconet Master Address:
00803716B4B4
< Back
Next >
Cancel
Help

Step 4 Press **Next**.


Recording Wizard: Test mode (Step 3 of 4)
System is Ready
Initiate Search/Record
Merlin Mobile is now ready to synchronize to the test piconet using Bluetooth Test-mode and start recording.
If your piconet is not currently established, please establish it now.
Or, you can establish it right after proceeding to the next page, while Merlin Mobile tries to synchronize to the piconet.
The following options will be used:
Synchronization Method: Test-mode
Frequency Band: Fixed-frequency mode
DUT's Transmit frequency: 2402 MHz
DUT's Receive frequency: 2404 MHz
Master address: 00803716B4B4
Advanced...
Press 'Next' to begin recording or 'Back' to return to the previous page.
< Back
Next >
Cancel
Help

Step 5 Press **Next**. Merlin Mobile then synchronizes with the

Master device and begins recording.

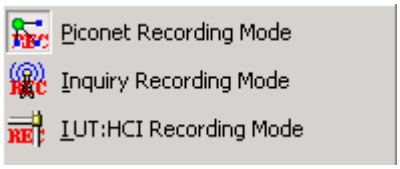

Recording Wizard: Test mode (Step 4 of 4)
Merlin Mobile is now attempting to synchronize and to record traffic on the test piconet using Bluetooth Test Mode.
Inquiring...
Select 'Cancel' to terminate the recording and to close the wizard.
< Back
Finish
Cancel
Help

6. Recording Options

The **Recording Options** dialog box provides an alternative method of setting up a recording to the Recording Wizard, described in the previous chapter. In this dialog box are all of the settings needed to make a recording. Once you have selected your recording options, you then select the recording mode by clicking the down-arrow on the Record button and selecting from the two mode options: Piconet and Inquiry. Merlin Mobile will then use the relevant Recording Options for the selected mode. For example, if you select **Piconet** recording mode, Merlin Mobile will use the options from the **Piconet** page in the Recording Options dialog box.

6.1 Recording Modes

Pressing the down-arrow on the Record button displays a menu with four Recording Modes:



Selecting one of these modes tells the analyzer what sets of Recording Options it should use when you begin a recording.

Note: Selecting a Recording Mode from the menu does not cause the analyzer to begin recording. To begin recording, you must press the Recording button itself.

Piconet recording

Selecting **Piconet**, configures Merlin Mobile to record piconet traffic using the parameters set in the Piconet page in the Recording Options dialog box. When you begin recording in this mode, Merlin Mobile will to try to synchronize to a piconet that matches the Piconet parameters set in the Recording Options. The recorded traffic is captured off-the-air.

Inquiry recording

This mode configures Merlin Mobile to record Inquiry traffic. When setting the Merlin Mobile to Inquiry recording, the system is ready to perform a Bluetooth 'General' or 'Dedicated' inquiry, according to the parameters

specified in the 'inquiry' page of the Recording Options. The recorded traffic would consist the transmitted packets as well as the responses received from Bluetooth devices in the area.

IUT:HCI mode

Configures the system to exclusively record HCI traffic from IUTs. This recording mode bypasses the analyzer: HCI traffic from the IUT is recorded directly by the analyzer software without going through the analyzer. This means that you can record HCI traffic even if the analyzer is not turned on.

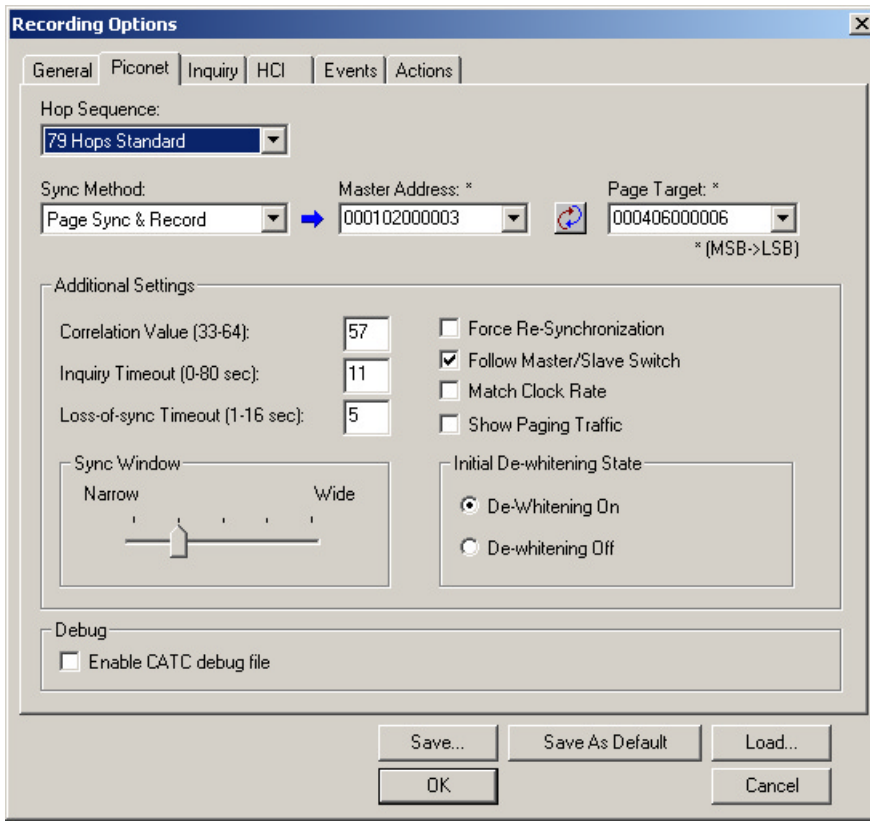
To record HCI traffic, first enable the recording of HCI traffic from IUTs. You do this in the HCI page of the Recording Options dialog. Then set the recording mode to something other than IUT:HCI. If you want to prevent the recording of HCI traffic from IUTs, disable it in the HCI page of the Recording Options dialog.

6.2 Opening the Recording Options Dialog Box

To open the **Recording Options** menu, click

on the Tool Bar or select **Recording Options** under **Setup** on the Menu Bar.

You see the **Recording Options** window. By default, the **Piconet** options page displays:



You will need to set options for each of the Recording Options pages. Generally, it is best to begin with the **General** and **Piconet** pages where you can set the type of recording, and then move on to the **Events** and **Actions** pages where you can set triggering events.

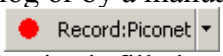
6.3 Recording Options - General

The General page controls the length of a recording and how it begins and ends. It is shown in the previous illustration. The General page display four boxes marked *Recording Type, Buffer Size, Trigger Position,* and *Options*.

Recording type

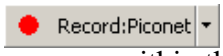
The **Recording Type** box presents options that control how Merlin Mobile begins and ends a recording. The options are: *Snapshot, Manual Trigger,* and *Event Trigger*.

Snapshot

A Snapshot is a fixed-length recording whose size is determined by the "Buffer Size" box in the Recording Options dialog or by a manual click of the Stop button. Recording begins by clicking 

on the Tool Bar and ends when either the selected buffer size is filled or you press the Stop button.

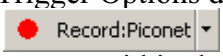
Manual Trigger

A Manual Trigger recording is a one that is manually begun and ended. Recording is begun by pressing 

on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer size. Recording ends when

is clicked on the Tool Bar or the Trigger button is pressed on the analyzer's front panel. If you press the Trigger button, recording will continue until the post-trigger memory has been filled.

Event Trigger

An Event Trigger recording is one that uses an event trigger to end the recording. Before recording begins, you define the event trigger in the Trigger Options dialog box. You begin the recording by clicking 

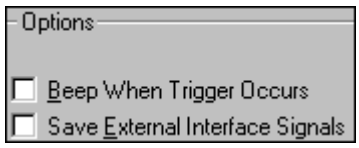
on the Tool Bar. Recording continues in a circular manner within the limits set by the buffer size. Once the trigger event occurs, some post-trigger recording occurs, then the recording ends.

Note In this mode, the recording can be stopped manually in the same way as for "manual trigger" mode.

Options

The Options box contains two options:

Beep When Trigger Occurs

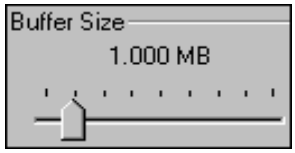


Will cause the PC to beep when a trigger event has occurred.

Save External Interface Signals

Will enable Merlin Mobile to record input signals from a breakout board as fields in a trace.

Buffer Size

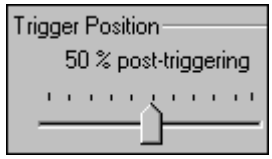


The Buffer Size box has a slide bar for adjusting the recording buffer size from 0.4 megabytes to 512 megabytes.

The Recording Type option determines how this buffer is used. Although there are 512 megabytes of physical memory in the analyzer, the efficiency of the recording ranges from 2:1 to 4:1 ratios of physical memory to actual Bluetooth traffic. Shorter Bluetooth packets yield a less efficient recording. The non-traffic portion of physical memory is utilized for control and timing information.

Note The scale is not linear and affords more granularity in the smaller buffer sizes.

Trigger Position



The Trigger Position slide bar sets the amount of post-trigger recording that Merlin Mobile will perform. It also allows adjustment of the location of the trigger within the defined buffer. You can adjust the Triggering Position between 1 and 99% post-Trigger. **Trigger Position** is available only when **Manual Trigger** or **Event Trigger** is selected as **Recording type**.

As an example, if the buffer size is set to 16MB, then for the following Trigger Position settings, the amount of pre- and post-Trigger data is

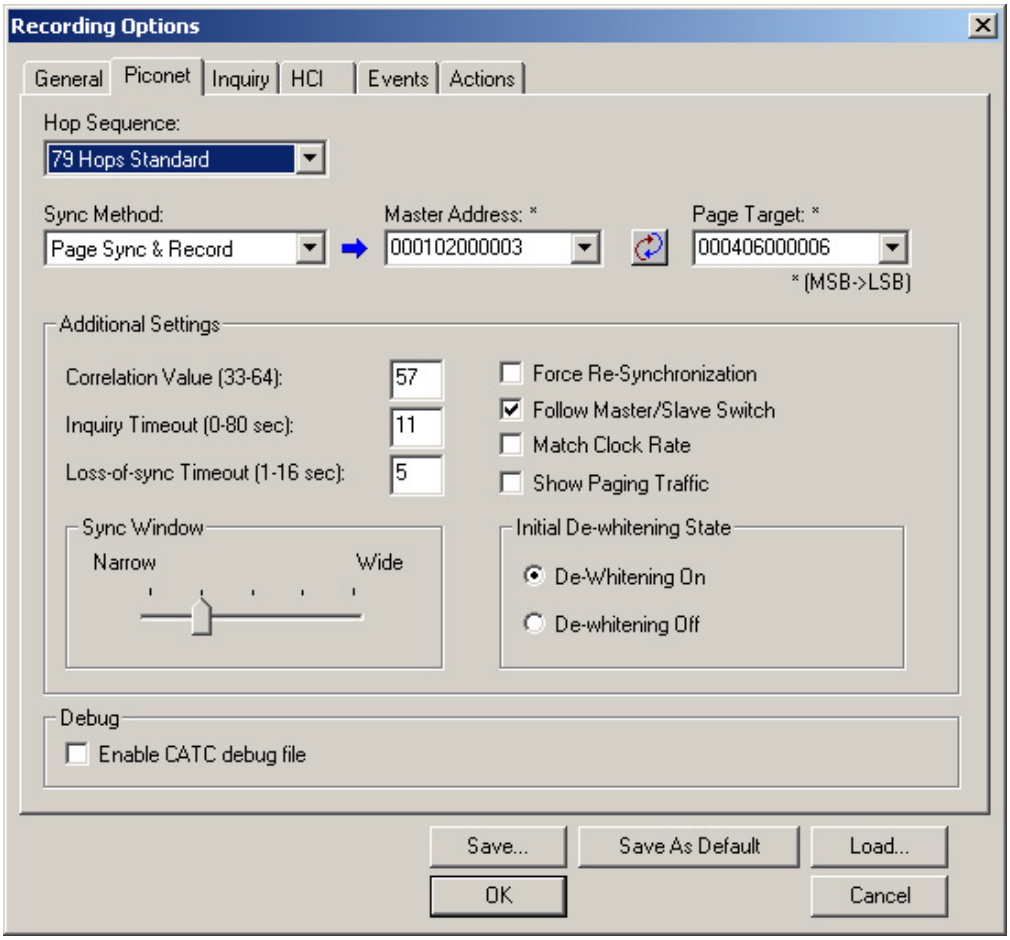
- 95% post-triggering: 0.8MB pre-trigger, 15.2MB post-trigger
- 75% post-triggering: 4MB pre-trigger, 12MB post-trigger
- 50% post-triggering: 8MB pre-trigger, 8MB post-trigger
- 25% post-triggering: 12MB pre-trigger, 4MB post-trigger
- 5% post-triggering: 15.2MB pre-trigger, 0.8MB post-trigger

Note When a Trigger occurs, recording continues until the post-Trigger amount of the buffer is filled.

6.4 Recording Options - Piconet

The Recording Options dialog box has two pages for configuring how Merlin Mobile records Bluetooth traffic: **Piconet,** which configures piconet recording sessions, and **Inquiry** which configures inquiry recording sessions.

For recording in Piconet mode, the **Piconet** page lets you specify the type of piconet you will be recording and how Merlin Mobile should synchronize and record the piconet. This window is divided into four boxes marked Hop Sequence, Sync Method, Additional Settings, and Debug.



Hop Sequence

The **Hop Sequence** menu presents the following three options:

- **79 Hops Standard** - This is the option used for most recordings.
- **Reduced Hop** - Restricts Merlin Mobile to five hop frequencies defined in the test mode specification of the Bluetooth Specification. When Reduced Hop or Single Frequency is selected, the Sync method is set to Test Mode and cannot be modified by the user.
- **Fixed Frequency** - Allows the transmit and receive frequency ranges to be specified. Selecting this option highlights the "DUT Xmit" and "DUT Recv" text boxes. When Reduced Hop or Single Frequency is selected, the Sync method is set to Test Mode and cannot be modified by the user.

Enter values into the two text boxes to the set the transmit and receive frequency ranges:

- DUT Xmit Freq, MHz (+2402) – Allows the setting of the transmit signal for the Device Under Test
- DUT Recv Freq, MHz (+2402) – Allows the setting of the receive signal for the Device Under Test

Sync Method

To record Bluetooth traffic, Merlin Mobile needs to synchronize to the piconet under observation. Merlin Mobile does not participate in the piconet and behaves as a passive listener. It needs, however, to communicate briefly with the devices in the piconet to learn the Master clock and frequency hopping sequence.

Sync Method options let you configure how Merlin Mobile synchronizes to the piconet under observation. There are three options:

- Sync and Record
- Passive Sync & Record
- Page Sync & Record

Note If the selected Hop Sequence is "Reduced Hop" or "Single Frequency," the Sync Method is set to "Test Mode" and cannot be modified by the user.

To the right of the Sync Method menu are two menus which let you select or enter address for the devices in the piconet:

Master Address - Presents a drop-down list of Master devices found previously. You can also enter address values in this box.

Page Target -- Presents a drop-down list of Page Target devices found previously. You can also enter address values in this box.

Between the two text boxes is the following button:

- Swaps the Master and Page Target addresses.

When to Use the Different Piconet Recording Modes

Page Sync & Record is the preferred option and should be used whenever possible. If Page Sync & Record can not be used, then Sync & Record should be used. Passive Sync and Record should be used only if the first two options can not be used.

Sync & Record

Sync and Record works just like "Page Sync and Record" except that Merlin Mobile takes its sync data directly from the Master instead of the Slave devices. With Sync and Record, Merlin Mobile conducts a General Inquiry to get hop frequency and clock information from the Master. Merlin Mobile then waits to detect piconet traffic from the Master device's piconet. When the piconet is established, Merlin Mobile is able to synchronize to the Master and begin recording. In contrast to "Page Sync and Record", "Sync and Record" can be run with or without an established piconet.

Note This mode can only be used to find master devices that support Inquiry Scan.

To perform a "Sync and Record", follow the steps below:

Step 1 Turn on the Bluetooth devices under observation, and set up the master device so it is ready to respond to Inquiry scan. For a typical recording, ensure that the Master and Slave device(s) are not yet connected.

Step 2 In the Modes tab under Recording Options, enter the Master Device's address.

Step 3 Start Merlin Mobile recording by pressing the Record button on the toolbar.

Step 4 When the analyzer is able to Sync up to the Piconet Master Clock, the Green **Sync** LED in the Merlin Mobile front panel will start blinking.

Step 5 Establish connection between the Bluetooth devices under analysis.

Step 6 When Merlin Mobile senses Piconet traffic, the Green **Sync** light goes ON solid, recording starts and the status bar in the bottom of the analyzer screen shows activity.

Recording may be stopped manually or when the recording buffer is filled.

Note After the Sync light starts blinking, a connection between the Bluetooth devices should be established within one (1) minute.

Passive Sync & Record

Passive Sync and Record is used in situations where the Master device and slave devices do not support Inquiry Scan mode. When selected, Merlin Mobile enters Inquiry Scan and Page Scan mode and waits for a page from

the Master device. When the piconet Master pages Merlin Mobile, Merlin Mobile obtains the information necessary for synchronization and then attempts to synchronize to the piconet controlled by that Master.

"Passive Sync and Record" is designed to be used with established piconets or *private device networks*.

Running "Passive Sync and Record" with Established Piconets

For most situations, "Passive Sync and Record" will be run after a piconet has been established. The steps are as follows:

Step 1 Establish a connection between two or more Bluetooth devices.

Step 2 Under General Recording Options, select "Passive Sync & Record."

Step 3 Under the Modes tab in Recording Options, enter the address for the piconet's master device.

Step 4 Make up an address for Merlin Mobile and enter it into the Page Target address in the Modes tab in Recording Options. Make sure you do not select an address for any other local device.

Step 5 Press the record button on the toolbar in Merlin Mobile to start a recording session.

Step 6 If necessary, have Master "discover" Merlin Mobile through a General Inquiry.

Step 7 From the Master device, initiate a page to Merlin Mobile's address. This action will enable Merlin Mobile to synchronize to the piconet. However, the analyzer will not complete the page sequence from the Master. This will cause the Master to time out in this request.

Step 8 At the end of this sequence, the green **Sync** light will go on solid, recording will begin and activity will be displayed on the status bar in the bottom of the analyzer screen.

Running "Passive Sync and Record" with Private Device Piconets

Because *private device networks* do not allow other devices to join the network, Merlin Mobile needs to temporarily assume the identity of a slave in the network in order to join that network. To do this requires disabling the slave and beginning the operation without an established piconet. The following steps show the process.

Step 1 Turn the Master device on and the slave device off. You need the slave device turned off so that Merlin Mobile can take its place in the piconet.

Step 2 Enter the slave's address into Merlin Mobile's "Page Target" field

in the Modes tab in the Recording Options dialog box.

Step 3 Run "Passive Sync and Record." The Master will then page the slave's address and Merlin Mobile will be able to sync.

Step 4 When Merlin Mobile synchronizes to the Master, turn the slave back on. When the Master re-pages the address the slave is admitted into the private network. Since Merlin Mobile is passive in this mode, the slave and Merlin Mobile do not conflict over the shared address. Merlin Mobile is then able to record the traffic between the Master and slave.

Page Sync & Record

"Page Sync and Record" is the recommended method of recording. "Page Sync and Record" should be implemented before a piconet is established. This mode causes Merlin Mobile to perform a General Inquiry and collect sync information from the specified slave device when it responds. Merlin Mobile then waits for the Master to begin paging the Slave devices. When paging begins, Merlin Mobile synchronizes to the Master and begins recording.

Note In order for this mode to work, the intended Slave must support "inquiry scan".

The following steps describe the simplest way to use this mode:

Step 1 Place both the "intended master" as well as its first "intended slave" into inquiry scan mode.

Step 2 Have Merlin Mobile perform a General Inquiry. You do this by pressing the BT Neighborhood button

Step 3 After the General Inquiry completes, the addresses will populate the menus marked **Master Device** and **Page Target**. Select or enter the addresses for both your Master Device and Page Target.

Step 4 Click **OK** at the bottom of the window to close the Recording Options dialog box.

Step 5 Press the

button found on Merlin Mobile's toolbar. After approximately 20 seconds, the "SYNC" light on the front of Merlin Mobile will begin to flash, meaning that Merlin Mobile has acquired all the information it needs to fully synchronize with the piconet about to be established. At this point, you should establish the piconet using the devices previously defined as master and slave.

Note Inquiry Timeout is configurable (0 to 80 seconds) in the Recording Options General page.

Step 6 When the piconet is established, the "Sync" light on the front of Merlin Mobile will change from flashing to solid, indicating that Merlin Mobile is fully synchronized to the piconet and is currently recording all traffic within that piconet.

Note If the "sync" light on the front of Merlin Mobile does not change from flashing to solid it means that Merlin Mobile did not synchronize with the piconet when it was established.

Additional Settings

Force Re-synchronization

"Force Re-Synchronization" forces Merlin Mobile to re-synchronize at the beginning of each "Sync & Record," "Passive Sync & Record," or "Sync & Record" operation. By default, "Force Re-Synchronization" is disabled (i.e., unchecked).

Unchecking the "Force Re-Synchronization" checkbox tells Merlin Mobile to use its existing data on Bluetooth devices, thereby bypassing the synchronization process and saving a few seconds from the beginning of the trace. If you know that Merlin Mobile's data is correct, you can uncheck this checkbox and cause Merlin Mobile to use the existing data. If the data is incomplete or incorrect, however, Merlin Mobile will automatically perform a refresh.

To examine Merlin Mobile's Bluetooth data, open Device List: **View >Device List**.

Follow Master/Slave Switch

If enabled, this option allows Merlin Mobile to follow a role switch between a Master and Slave. This capability allows Merlin Mobile to keep track of changes in a device's role when it changes from one role to another.

Merlin Mobile is able to follow a role change by listening to the Slave device's Bluetooth clock and hop frequency as soon as it becomes a Master.

Match Clock Rate

Match Clock Rate is a useful option if the Master device's clock is inaccurate. Match Clock Rate causes Merlin Mobile to do a General Inquiry to determine the Page Target's clock rate prior to synchronizing to the piconet. If unchecked, Merlin Mobile will begin piconet synchronization without first doing a General Inquiry.

This option only works with Page Sync and Record mode.

Show Paging Traffic

Show Paging Traffic causes Merlin Mobile to capture paging traffic between the Master and Page Target devices. This option is used only with Page Sync and Record Mode.

Correlation Value (33-64)

This value tells Merlin Mobile how many bits in the sync word of each received packet must be matched in order for Merlin Mobile to consider the packet valid and start recording.

It is recommended that the Correlation Value be set to 57 bits.

Inquiry Timeout (0-80 secs)

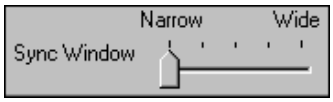
Default value is 20 seconds.

This value specifies how long Merlin Mobile should perform the Inquiry process for the General (unlimited) and Dedicated (limited) recording modes. After the specified time has elapsed, Merlin Mobile will illuminate the trigger light on the front of the analyzer.

Loss of Sync Timeout (1-30 secs)

This value specifies the amount of time that Merlin Mobile will wait for piconet traffic before determining that synchronization has been lost.

Sync Window



The Sync Window slide bar controls the amount of time that Merlin Mobile should wait between receiving an Inquiry Response (which will cause the Sync LED to blink) and detecting Master-Slave piconet traffic (which will cause the Sync LED to turn solid.)

A "Narrow" setting means that the wait time will be minimal, a "Wide" setting means it will be "maximal." The default is "Narrow" and this is suitable for most recordings. However, if significant drift occurs between Merlin Mobile's clock and that of the Master, Merlin Mobile may not be able to sync properly to the piconet. Under these conditions, you should move the slide bar towards the "Wide" Setting. The slide bar has five discrete settings.

After sync is established, Merlin Mobile will remain in sync as long as there is piconet traffic.

Debug

Enable CATC debug file

Checking this box enables the creation of a file that can be used by CATC Support to aid in debugging. This option should always be disabled unless you are requested to enable it by CATC personnel.

6.5 Recording Options - Inquiry

The **Inquiry** page configures how Merlin Mobile records Inquiry traffic. Two main options are presented in the **Sync Method** drop-down menu: General (Unlimited) Inquiry and Dedicated (Limited) Inquiry. These options tell Merlin Mobile what kind of Inquiry traffic it should expect to record.

This page includes settings only for Inquiry recording and BT Neighborhood.

General (Unlimited)

"General" means "General Inquiry" and is used to search for ALL Bluetooth devices that are within range, for the amount of time specified in the Inquiry Timeout field. Completion of the inquiry process is indicated by illumination of the "trigger" light on the front of the analyzer. All responding packets will be displayed when data upload from the analyzer completes.

Dedicated (Limited)

"Dedicated" means a specific class or group of Bluetooth devices (designated by the DIAC field of the Recording Options dialog). Selecting "Dedicated" causes Merlin Mobile to search for all devices from a specific class or group that are within range, for the amount of time specified in the Inquiry Timeout field. Completion of the inquiry process is indicated by illumination of the "trigger" light on the front of the analyzer. All responding packets will be displayed when stop is selected.

BT Neighborhood

These options configure how the BT Neighborhood command behaves. BT Neighborhood is a utility that performs an Inquiry and then lists the local devices that it discovered.

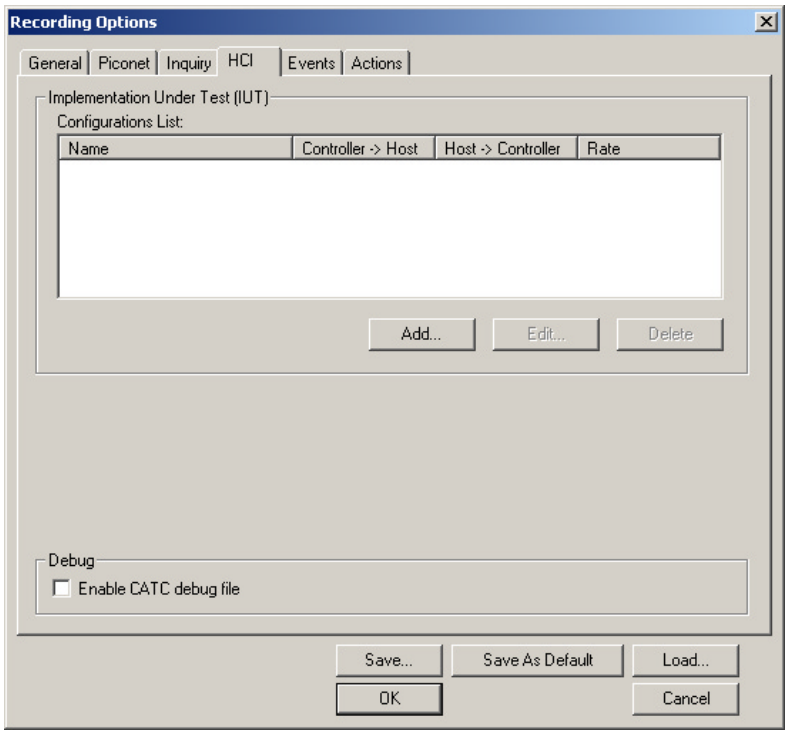
- **Use Default settings** -- Sets the analyzer to record a General Inquiry with an Inquiry Timeout of 11 seconds.
- **Match 'Inquiry' Recording Settings** -- Sets the analyzer to use the settings you chose above under Hop Sequence, Inquiry Type, and Additional Settings.

Debug

Enables the creation of a file that can be used by CATC Support to aid in debugging.

6.6 Recording Options - HCI

The HCI property page lets you include HCI traffic from IUTs into the trace. HCI traffic consists of commands and other traffic that are sent by the IUT to generate Bluetooth traffic. By default, this option is disabled - meaning that HCI traffic is not shown in the trace.



HCI Traffic from the IUTs is captured by the analyzer application using an HCI probe (provided by CATC) that is connected directly to the IUT hardware. In a typical setup, the HCI commands and data to transmit are passed from the Bluetooth application to the Bluetooth baseband (Host to Controller), while events and data that was received are passed from the Bluetooth baseband to the Bluetooth application (Controller to Host).

To capture the data, the HCI Probe should be connected to the respective 'Host to Controller' and 'Controller to Host' lines. When the recording of the IUT's HCI is enabled and the application starts a recording, the serial data is captured as incoming serial data. For this, up to two COM ports should be configured for each IUT.

HCI Window Layout

The HCI page displays a Debug checkbox, a Configurations List that is made up of IUTs that were added via the **Add** button, and buttons labeled **Add**, **Edit**, and **Delete**.

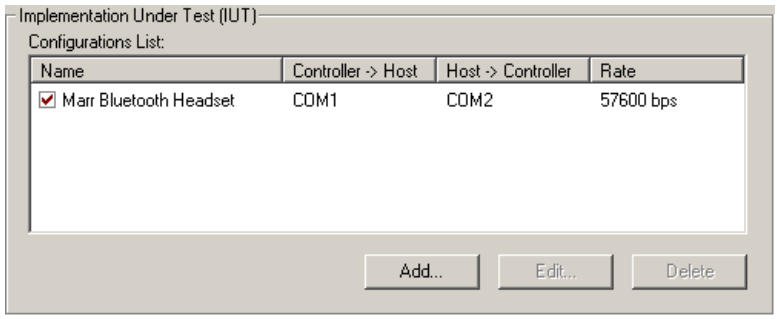
Debug

Enables the creation of a file that can be used by CATC Support to aid in debugging.

Configurations List

The Configurations List displays the COM settings for the ports used to connect the IUT to the host PC.

The Configurations List allows you to manage as list of up to three IUTs to be recorded and set the parameters for each one. It also allows you to enable or disable a specific IUT from being recorded. The settings are stored in the recording options file, like the rest of the recording options.



The Configurations List is made up of the following fields:

- **Name** - Symbolic name of the IUT given by the user, for easy identification.
- **Controller => Host** COM port - The port that is used for the capturing of the up- link traffic.
- **Host => Controller** COM port - The port that is used for the capturing of the down-link traffic.
- **Rate** - the bits per second rate the COM ports are configured for.

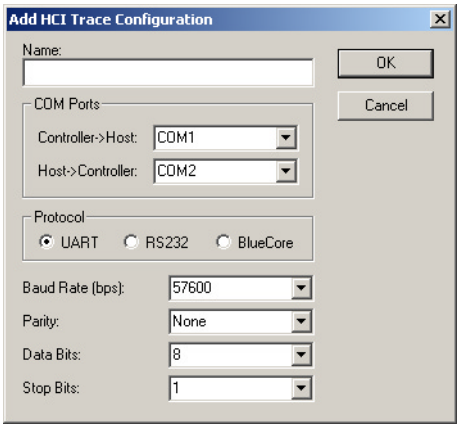
The list displays three possible states for each one of the entries:

- **Enabled** - The HCI traffic from the IUT is going to be recorded.
- **Disabled** - The HCI traffic from the IUT is not going to be recorded.
- **Invalid** - The analyzer failed in opening the COM port for accessing the IUT, with the listed parameters. In this case, you should refer to Windows configuration of the COM ports or check

whether the same COM port(s) is (are) used by other applications in the host machine or that the parameters are set correctly.

Add ...

The **Add** button lets you add devices to the Configurations List. Clicking **Add** causes the following dialog box to open:



Name - Symbolic name for easy identification of the device and connector.

Controller -> Host - COM port used for monitoring the HCI traffic from the application to the bluetooth baseband.

Host -> Controller - COM port used for monitoring the HCI traffic from the Bluetooth baseband (Controller) to the application (Host).

Rate - Sets the maximum rate in bits per second (bps) that you want data to be transmitted through this port.

Data Bits - Changes the number of data bits you want to use for each character that is transmitted and received. The computer or device you are communicating with must have the same setting that you choose here. Most characters are transmitted in seven or eight data bits.

Parity - Changes the type of error checking you want to use for the selected port. The computer or device you are communicating with must have the same setting that you choose here. You must choose one of the following:

- **None** - No parity bit will be added to the data bits sent from this port. This will disable error checking.
- **Even** - Parity bit is set to 1 if it is needed to make the number of ones in the data bits even. This will enable error checking.
- **Odd** - Parity bit is added if it is needed to make the number of ones in the data bits odd. This will enable error checking.
- **Mark** - Parity bit is added but is always set to 1.

Stop Bits - Changes the time between each character being transmitted (where time is measured in bits).

Edit

The Edit button reopens the **Add HCI Configurations** dialog box so you can edit your settings. Be sure to select an entry in the HCI Configurations list before clicking **Edit**.

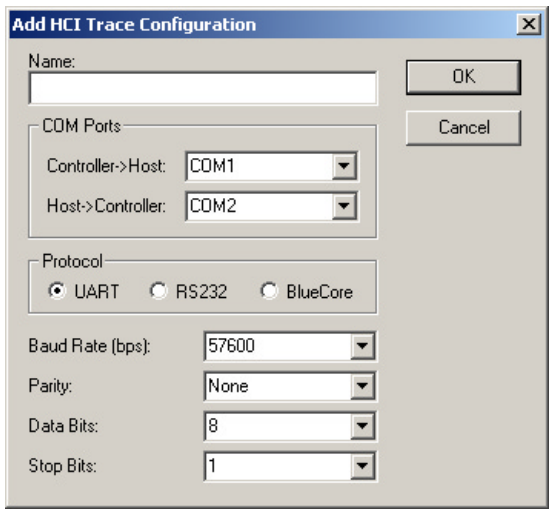
Delete

The Delete button allows entries to be deleted from the Configurations List.

6.7 Recording HCI Traffic

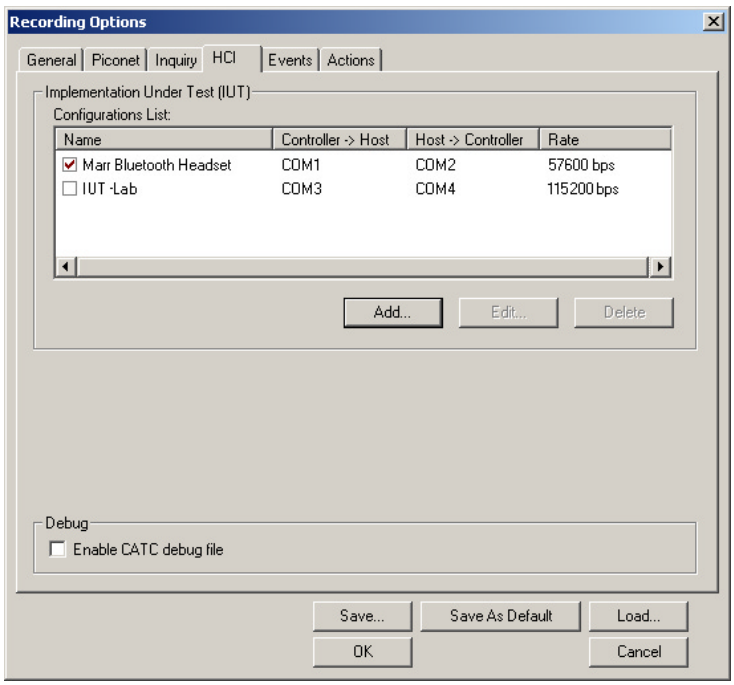
To record HCI traffic from an IUT, enter data in the HCI window.

Step 1 In Recording Options, go to the HCI page, and click **Add**. The Add HCI Trace Configuration dialog appears.



Step 2 Enter the pertinent data in the data fields, and click OK. The HCI configuration is shown in the HCI page of Recording

options.



To edit an entry in the Configurations List,

Step 1 In the HCI page of Recording Options, click **Edit**.The Edit HCI Trace Configuration dialog appears.

Step 2 Change the data in the data fields according to your desired changes, and click **OK**. The changes are reflected in the Extern page of Recording Options.

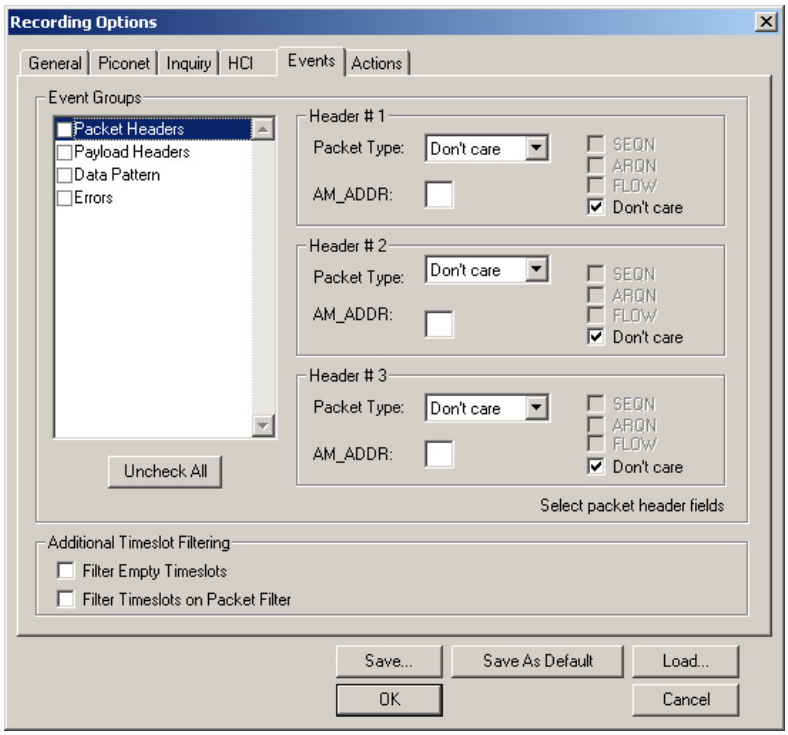
6.8 Recording Options - Events

If you have selected **Event Trigger** mode under the **General** tab in the Recording Options screen, you may now select specific Bluetooth events using the **Events** tab on the **Recording Option** Screen. You can also use the **Actions** tab to define specific event sequences that will trigger Merlin Mobile to record a Bluetooth session.

In addition, the **Events** and **Actions** screens allow you to specify which packets you want to include or exclude from the recording.

- Click the **Events** tab on the **Recording Options** screen.

You see the **Event Groups** window:



The Event triggering and filtering options allow you to set event conditions for errors and/or a variety of packet characteristics.

Clicking a check box causes further options to display in the right side of the window.

Additional Timeslot Filtering

By default, Merlin Mobile records frequency hop and timestamp information for all time slots in the Piconet under analysis, regardless of whether the time slot contained a Bluetooth packet. This means that in instances where there is little piconet traffic, Merlin Mobile will display row after row of empty packets -- each representing an empty time slot. Through the use of timeslot filtering, these empty packets can be filtered out. Filtering out this information has the benefit of freeing memory so that more traffic can be recorded.

Filter Empty Slots

If "Filter Empty Slots" is checked, Merlin Mobile will exclude all empty time slots from a recording except for those that lie immediately in front of Bluetooth communications packets. These remaining empty packets are preserved to give timestamp and frequency hop reference data to the packets that follow.

Filter Slots on Packet Filter

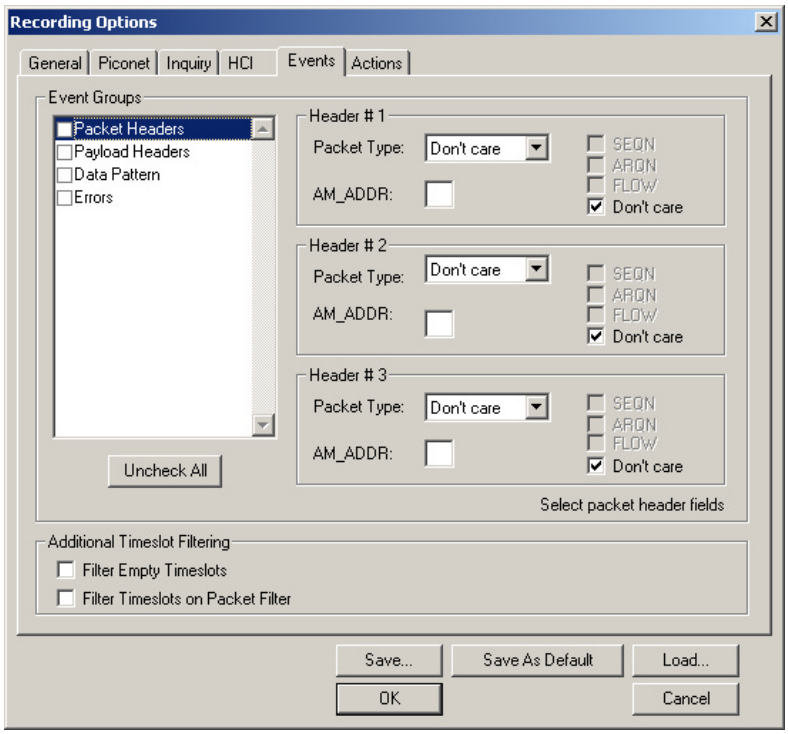
If filters are used to exclude FHS, DM1 or other packets, Merlin Mobile will exclude these packets from a trace and mark their locations with empty packets. The result can be rows and rows of empty packets. The option "Filter Empty Slots" will not exclude these empty slots because they lie immediately in front of Bluetooth communications packets - even though those packets were not recorded. To eliminate these empty packets, select "Filter Slots on Packet Filter."

Packet Headers

Clicking "Packet Headers" opens three sets of check boxes and menus on the right that represent fields within packet headers: Packet Type, Active Member Address, Flow Control, Acknowledgment, and Sequence Number.

- Select **Packet Headers** under **Event Groups.**

  You see the **Packet Headers** window:



Packet Type

The Packet Type drop down menu lets you select the following packet types for filtering or triggering: NULL, POLL, FHS, DM1, DH1, HV1, HV2, HV3, DV, AUX1, DM3, DH3, 1100, 1101, DM5, or DH5.

Select "Don't Care" if you want Merlin Mobile to ignore this field.

AM_ADDR

(Active Member Address) The AM_ADDR is a three bit slave address. To select packets from a particular slave device for filtering or triggering, enter an address into the AM_ADDR text box. You can target up to three devices using the three text boxes.

SEQN, ARQN, and Flow Control Bits

To set event conditions on SEQN, ARQN, and Flow control, uncheck "Don't Care." Unchecking "Don't Care" sets the event condition to SEQN=0 AND ARQN=0 AND Flow=0. This action also puts a checkmark in the box marked "Packet Headers." A checkmark next to SEQN, ARQN, or Flow changes the value of this field from zero to one. For example, if SEQN is checked, the event condition becomes "SEQN=1 AND ARQN=0 AND Flow=0.

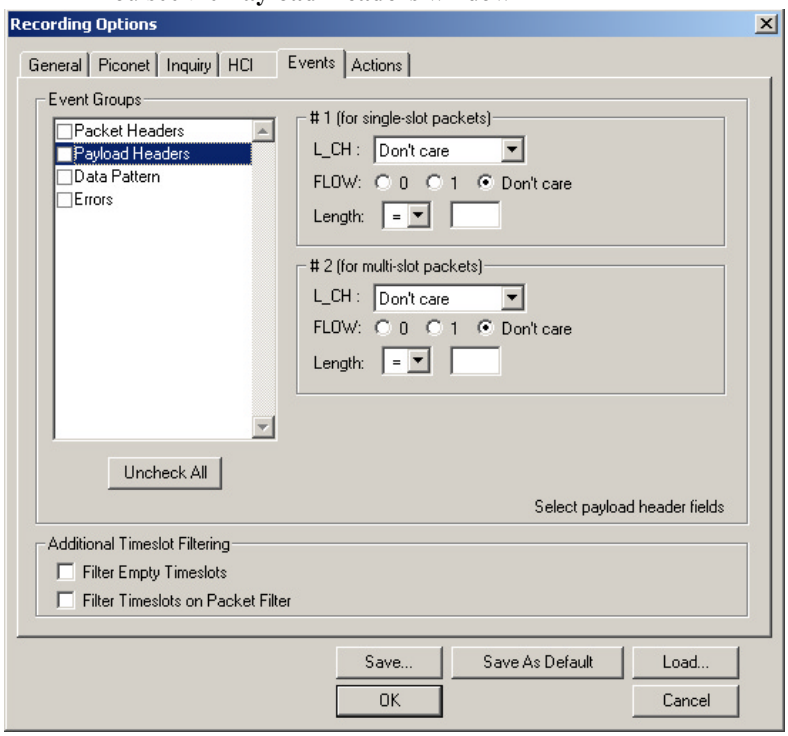
To cause Merlin Mobile to ignore this set of check boxes, choose "don't care."

Payload Headers

Clicking "Payload Headers" causes a series of options to display on the right for setting conditions on payload headers. You will see two sets of options - one for single slot packets such as DM1 packets and a second for multi-slot packets such as DM3 packets. Within each set is a menu for the Logical Channel and sub-options for Flow Control, and Payload length. These latter two options allow you to modify searches based on the Logical Channel. An example would be "Trigger on a start L2CAP message whose flow control bit is 1 and whose data field length is less than 20."

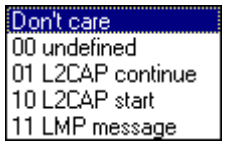
- Select **Payload Headers** under **Event Groups.**

You see the **Payload Headers** window



L_CH (Logical Channel)

The "L_CH" drop down menu presents five options for setting conditions on the Logical Channel:

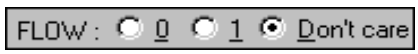


- Don't care
- 00 Undefined
- 01 L2CAP continue
- 10 L2CAP start
- 11 LMP message

Select "Don't care" if you do not want to set conditions on Logical Channel.

Flow

Three "radio buttons" are presented for setting conditions based on Flow control:

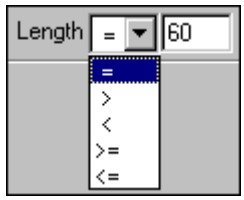


- 0
- 1
- Don't care

Flow works in conjunction with the Logical Channel (L_CH) menu - you select an option from the L_CH menu and then select an option under Flow.

Select "Don't care" if you do not want to set conditions on Flow control.

Length (in bytes)

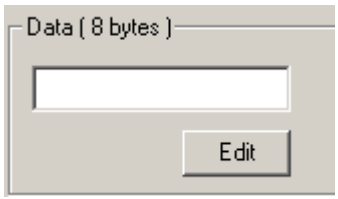


Using both the drop down menu and the text box, you can set conditions based on data field length. The maximum length for a single slot packet is 29 bytes. The maximum length for multi-slot packets is 339 bytes.

The drop-down menu gives you options for selecting operators such as "greater than" and "equal to." The text box to the right of the drop-down menu lets you enter values.

The Length option works in conjunction with the Logical Channel (L_CH) menu - you first select an option from the L_CH menu and then select an option under Length.

Data Patterns



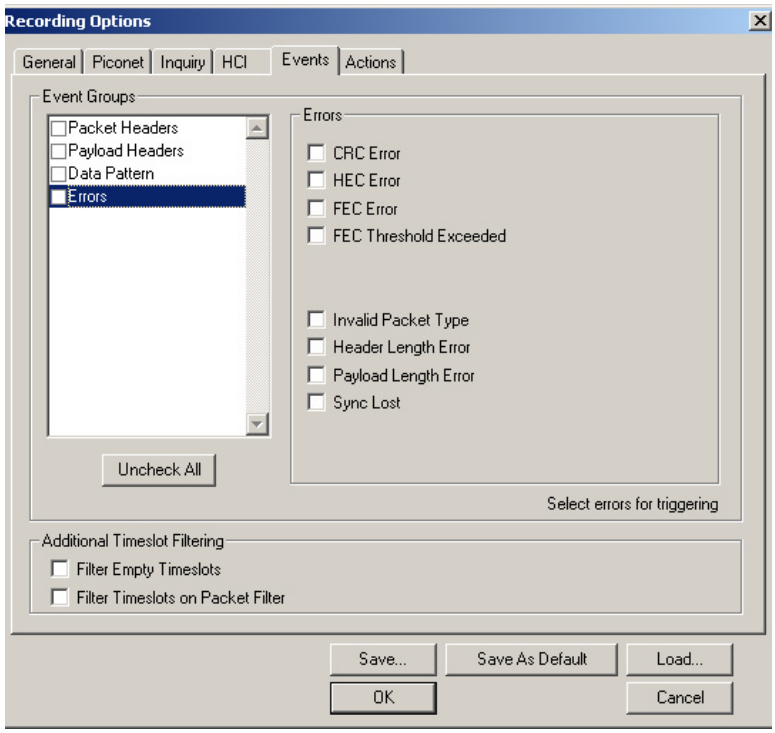
Clicking "Data Patterns" causes a text box to appear for entering patterns to be matched in the raw payload data. Patterns of up to eight hexidecimal bytes can be entered.

Errors

Clicking "Errors" causes check boxes to appear for setting conditions for triggering or filtering based on packet/signaling/protocol errors. You can select one or a combination of errors.

- Select **Errors** under **Event Groups.**

You see the **Errors** window:



Use any combination of the listed packet/signaling/protocol errors as a Trigger.

CRC Error

A CRC error in the packet data payload of the previous Bluetooth data packet.

HEC Error

An HEC (header error check) error in the packet header for the previous Bluetooth data packet.

FEC Error

An uncorrectable FEC (Forward Error Correction) error in the packet header for the previous Bluetooth data packet.

Threshold Exceeded

Indicates that the number of single-bit FEC errors detected since the current recording started has exceeded the specified value.

Invalid Packet Type

An invalid value was detected in the 'packet type' field of the packet header for the previous Bluetooth data packet.

Header Length Error

Indicates that a received Bluetooth data packet was terminated before all bits of the packet header were received.

Payload Length Error

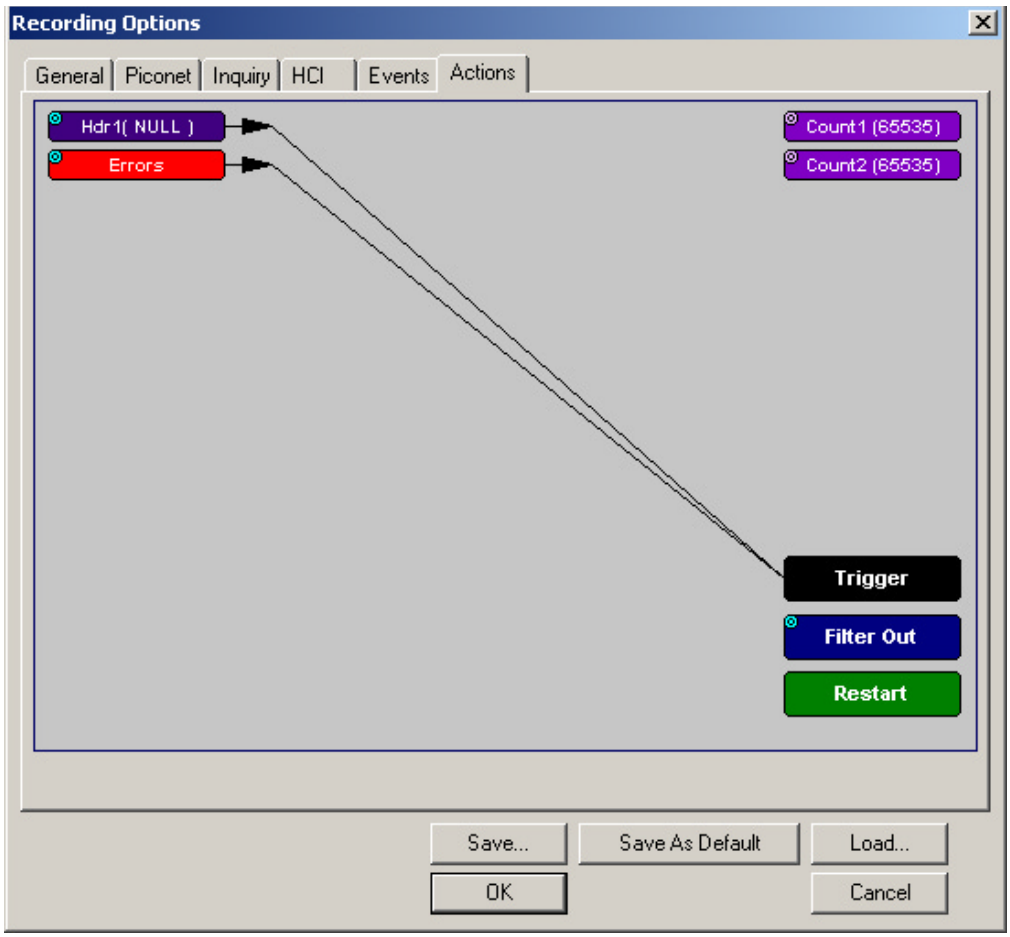
Indicates that the payload of a received Bluetooth data packet was either longer than expected, or that a Bluetooth data packet terminated before the expected end of the payload data.

Sync Loss

When set, indicates that a loss of piconet synchronization occurred during the frequency slot prior to this slot.

6.9 Recording Options - Actions

The **Actions** screen allows you to specify the type of action that Merlin Mobile should perform when it encounters the events specified in the **Events** window.



Action Buttons - Their Functions

The **Action** buttons in the right side of the window provide the means of setting triggers, filters, and restarts. To set an action, you simply drag your mouse from an Event to an Action. As described further on, this movement will link the two via an arrow.

Trigger

The **Trigger** button enables event triggering.

Filter In/Out

The **Filter In/Out** button allows events to be filtered in or out of the recording. Filtering provides a useful method of excluding data from the trace so you can conserve recording memory.

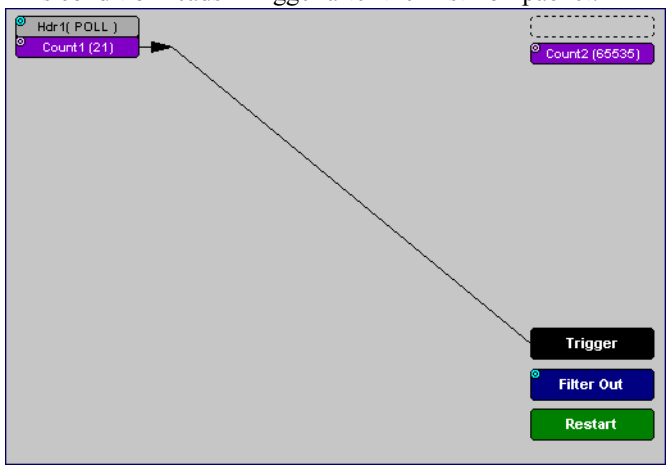
Restart

The **Restart** button causes the two counters Count1 and Count2 to be reset to zero. It also causes the search for *event sequences* to restart. Event sequences are sequences of events that trigger the end of the recording. Restart buttons provide you with a way of saying "If you see a sequence of A, B, C, and D, then trigger. However, if you see *X* anywhere during the sequence, restart your search."

Count1, Count2

Count1 and Count2 are counters for specifying how many events must occur before an event can cause a trigger. Counters allow conditions to be made such as "Trigger after the 21st Poll packet" (see screenshot below).

The Actions window showing a condition based on a Poll packet and a counter. This condition reads "Trigger after the 21st Poll packet."



Connecting Events to Counters

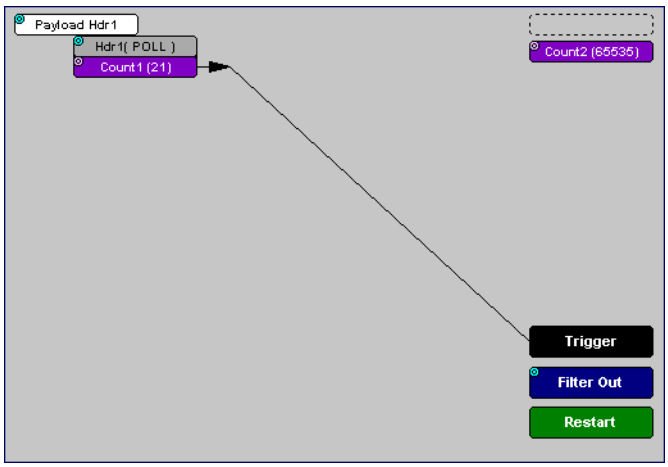
To connect an event to a counter, click an Event button, then click one of the two counter buttons. The Counter will reposition itself immediately below the event. A line will the connect the counter to the Trigger button.

This latter connection between the Counter button and the Trigger button occurs because counters always work in association with triggers. Counters act as assistants to triggers.

Setting Multiple Conditions with Counters

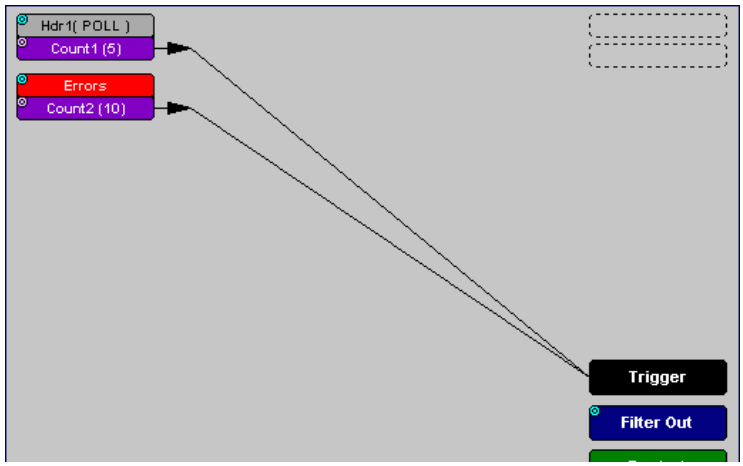
You can create multiple event conditions by linking a counter to multiple events or by linking two counters to two or more events.

Linking Multiple Events to One Counter - When two or more Events are strung together and then connected to a counter, the event button that is touching the counter gets counted. The example below reads "Trigger after you see a sequence of a packet with the specified payload followed by a 21 null packets."



Linking Two Events to Two or More Counters - If an Event is linked to **Count1** and a second event is linked to **Count2**, it creates an "or" statement. This statement reads "Trigger when Count1 OR Count2 has reached their specified values."

This example reads "Trigger when Count1 has counted 5 Poll packets or Count2 has counted 10 errors."



Blue Dot Menus

Count1, **Count2** and a few other buttons in the **Actions** window have blue dots in their top left-hand corners that indicate the presence of context-sensitive menus. These menus let you set the button's values and/or operations. Click the left mouse button on a dot to open the menu.

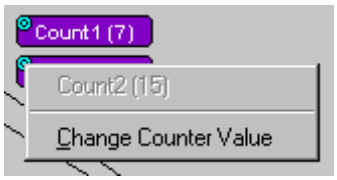
Counters Blue Dot Menu

The **Count1** and **Count2** blue dot menus allow the value of their counters to be changed. The value you specify here tells Merlin Mobile how many instances of an event must take place before a trigger occurs. The counter can be set between 1 and 65,535.

To set a Counter,

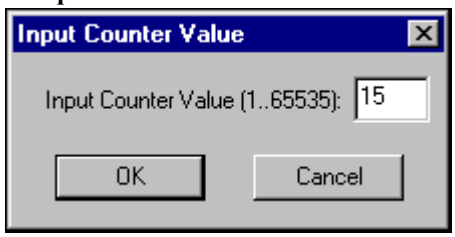
Step 1 Click on the blue dot in the upper left corner of the **Count** button.

You see the **Change Counter Value** menu:



Step 2 Click **Change Counter Value**

You see the **Input Counter Value** menu



Step 3 Enter an input value to tell the Analyzer how many times this event must occur before triggering the end of a recording

Step 4 Click **OK**.

Filter Out/In Blue Dot Menu

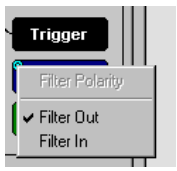
The **Filter Out/In** button toggles between "**Filter Out**" and "**Filter In**".

- **Filter In** records ONLY those packets related to the specified event.
- **Filter Out** records all packets EXCEPT those related to the specified event.

To filter an event in or out of a recording,

Step 1 Click the blue dot on **Filter Out**. (Note: the button may say **Filter In** depending on the last action specified.)

You see the **Filter Out/In** menu:



Use this menu to toggle the selection between **Filter Out** and **Filter In**.

Step 2 Select "**Filter In**".

The button changes to read "Filter In".

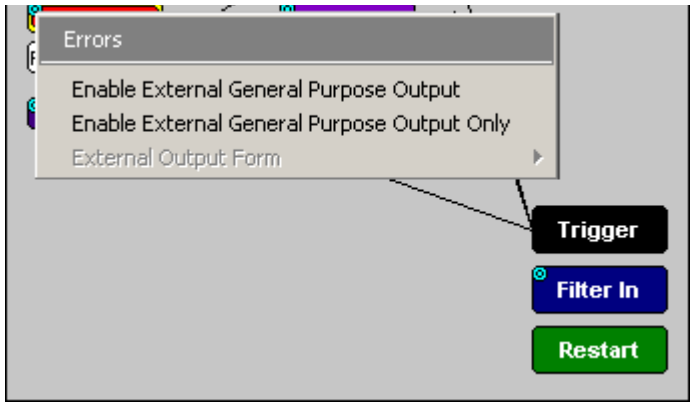
Blue Dot Menus for the Event Buttons

The **Errors** button and the first Headers button (marked "**Hdr1**") have the same Blue Dot menus. These menus allow Merlin Mobile to trigger external output.

To enable or disable external trigger output,

Step 1 Click the Blue Dot on an Event button such as **Hdr1** or **Errors**.

A menu similar to the one below will open. Your menu may say "Disable" instead of "Enable."



Step 2 Select "**Enable External Trigger Output**" (or "**Disable External Trigger Output**" if that is the choice presented.)

If you have chosen "**Enable External Trigger Output**", a small arrow will appear on the right side of the button. This arrow indicates that a condition has been set for creating an external output signal. Choosing "**Disable External Trigger**" will cause the arrow to disappear.

Enabling High Pulse, Low Pulse or Pulse Toggle Signal Outputs

Once External Trigger Output has been enabled, you can configure the output signal to one of three formats:

Pulse High - This is the default format. The Pulse High setting causes the Analyzer to transmit a 5 volt, 16.66 nanosecond signal.

Pulse Low - This format causes the Analyzer to transmit a -5 volt, 16.66 nanosecond signal.

Toggle - This format causes the Analyzer to transmit a signal that will toggle with each trigger event between a continuous 5 volt signal and a continuous -5 volt signal.

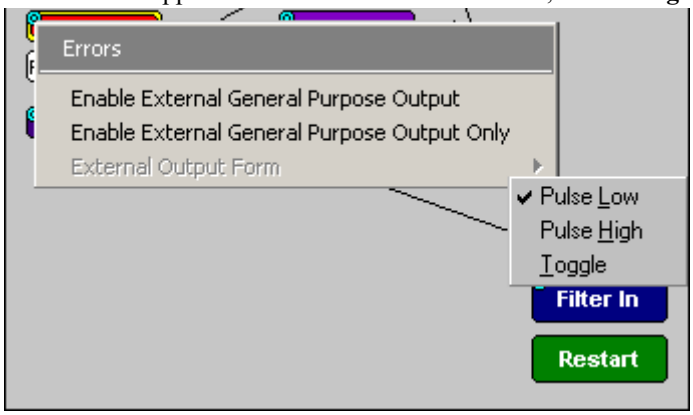
To configure the output signal,

Step 1 Click the blue dot on an Event button that has a small arrow attached to it like the one shown above.

A Blue Dot Menu will open. "**External Trigger Form**" should be a choice available. If it is not, you will need to choose "**Enable External Trigger**" and then reopen the menu.

Step 2 Choose "**External Trigger Form**"

A menu will appear with choices for "**Pulse Low**", "**Pulse High**", and "**Toggle**".



Step 3 Choose an option not currently selected.

The menu closes.

Step 4 Reopen the menu.

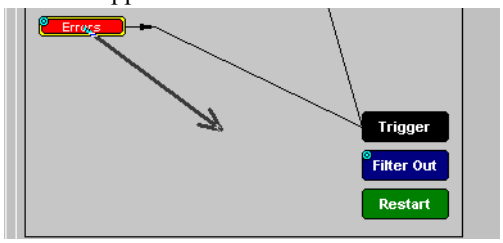
Note that your new selection is now checked.

Elastic Arrow

Elastic arrows allow you to associate Events, Counters, and Actions. To make an association,

Step 1 Click the left mouse button on an Event button such as **Hdr1** or **Errors**.

The elastic arrow appears.



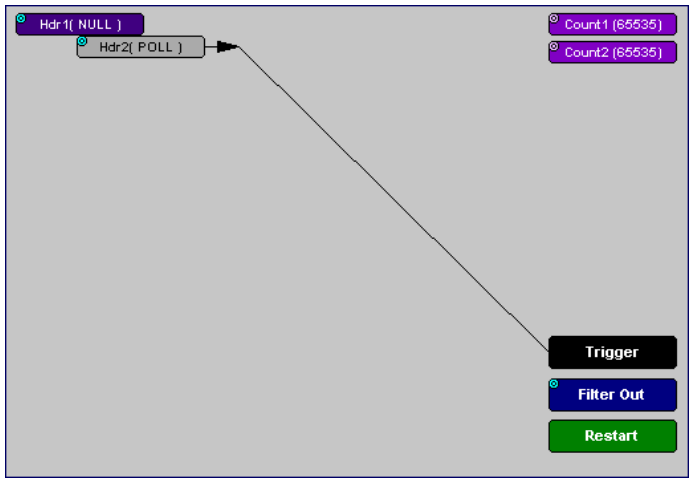
Step 2 Drag the arrow to the desired Action button.

Step 3 With the pointer over an Actions button, click again the left mouse button again.

The arrow is replaced with a black line connecting the Event button to the Action button.

Event Sequencing

If you drag your mouse from one event button to another, you will create a compound condition known as an *Event Sequence*. An event sequence is a condition that says "Trigger when you see the following sequence of packets." The example below may help to clarify.



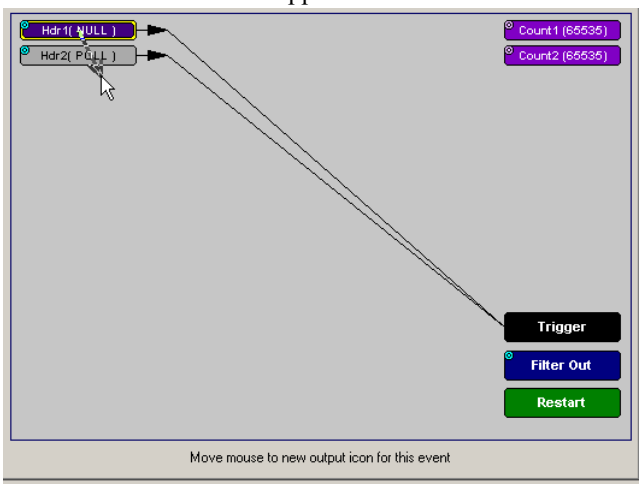
This example means "Trigger when you see a packet with an Null Header followed by a packet with a Poll Header."

To create an event sequence, perform the following steps:

Step 1 Select two events from the Events window

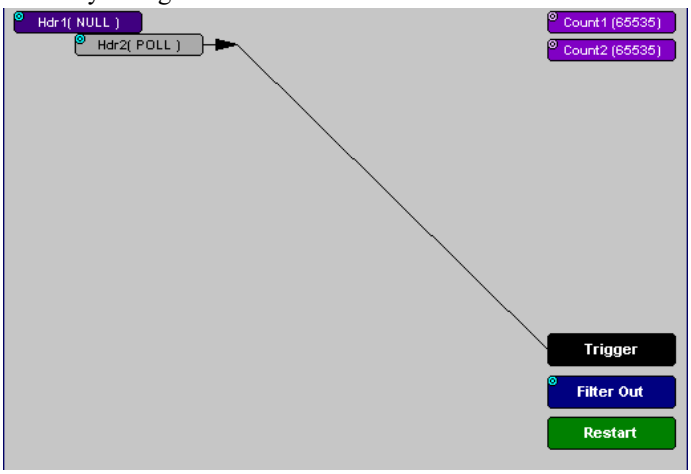
Step 2 Open the Actions window and click on one of the two Event buttons.

An elastic arrow should appear.



Step 3 Click on the other event.

The arrow should connect to the second button and the second button should instantly change locations to the center section of the window.



6.10 Saving Recording Options

To complete your Recording Options settings, use the features at the bottom of the **Recording Options** screen. These features remain the same no matter which of the three Recording Options screens you are working in.

- Click **Save** to save the currently specified Recording Options for use in future recording sessions. Any file name can be specified, though use of the **.rec** is recommended; if no extension is specified, **.rec** is added by default.
- Click **Load** to load a previously saved ***.rec** file, thus restoring a previous set of Recording Options.
- The **Save as Default** function is equivalent to the **Save** function, specifying the file name **default.rec.** Whenever you start up the Analyzer, it automatically loads the **default.rec** file if one exists.
- Click **OK** to apply any changes and close this dialog box.
- Click **Cancel** to cancel any immediate changes you have made and exit the Recording Options menu.

6.11 Recording Bluetooth Traffic

To start recording Bluetooth traffic once the appropriate Recording Options have been set,

Step 1 Select **Start** under **Record** on the Menu Bar

OR

Click on the Tool Bar.

Your recording session can continue until it has finished naturally or you may need to stop manually by clicking on the Tool Bar, depending on how you set the Recording Options.

To manually stop recording,

Step 2 Select **Stop** under **Record** on the Menu Bar

OR

Click on the Tool Bar.

Note The manual Stop Recording feature is primarily of use when recording low-volume traffic, which can take a long time to fill the recording buffer.

When the recording session is finished, the bus traffic is saved to the hard drive as a file named **data.tfb** or whatever name you assign as the default filename.

If you have enabled the recording is serial HCI traffic from IUT, then a second trace file is created called data_hci.tfb.

To save a current recording for future reference,

Step 3 Select **Save As** under **File** on the Menu Bar.

OR

Click on the Tool Bar.

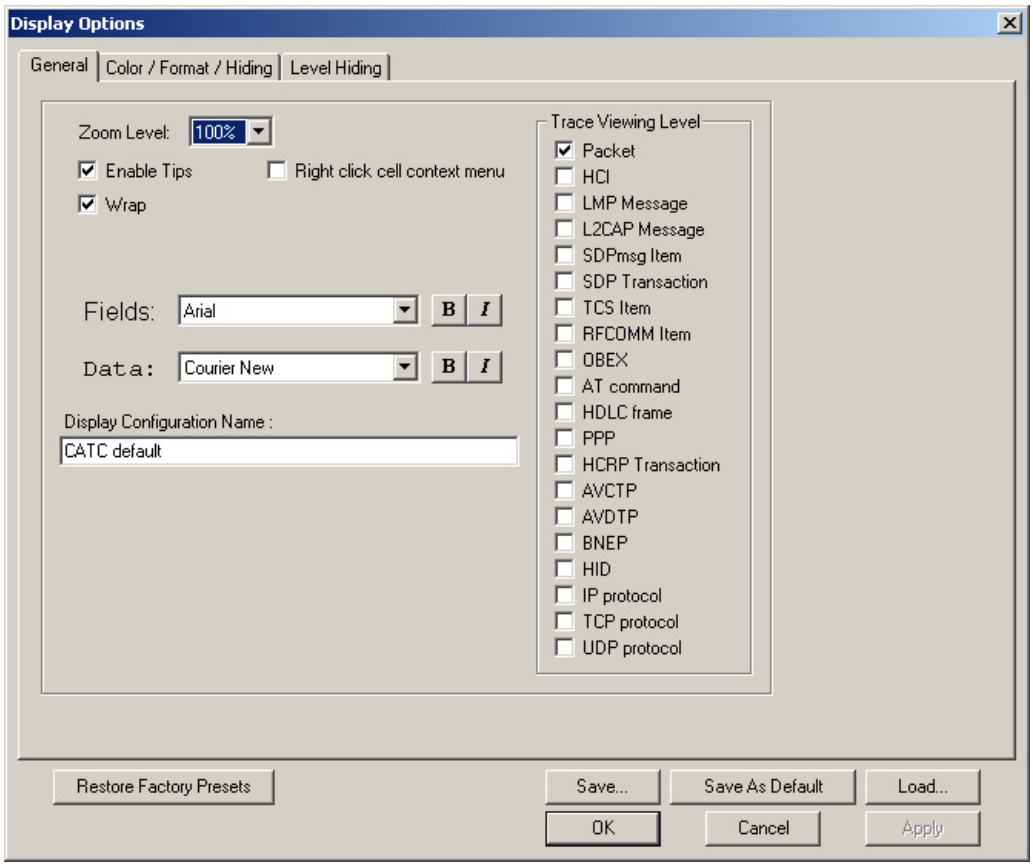
You see the standard **Save As** screen.

Step 4 Give the recording a unique name and save it to the appropriate directory.

7. Display Options

Use the **Display Options** menu to specify the way CATC Trace information is displayed.

From the **Setup** menu, select **Display Options**.



7.1 General Display Options

Use the General Display Options to specify the basic appearance of a Trace view.

- **Zoom Level**: Adjustable in discrete increments from 10% to 200% percent.
- **Enable Tips**: Select to enable Tool Tips with explanation text to pop up when you position your cursor over various fields in the Trace View.
- **Wrap**: Causes packets to wrap within the window if their length exceeds the width of the window.
- **Right click cell context menu**: Activates the right mouse button for opening cell context menus.
- **Trace Viewing Level**: Allows you to select the hierarchical level at which traffic is displayed.
- **Fields**: Configures the appearance of field text within the trace.
- **Data**: Configures the appearance of data within the trace.
- **Display Configuration Name**: Comment field associated with the ***.opt** file containing the current Display Options values. You can also create and store your unique Display Options for future use.

To create a new Display Options file, follow these steps:

Step 1 Enter a comment for the new file in the **Display Configuration Name** field.

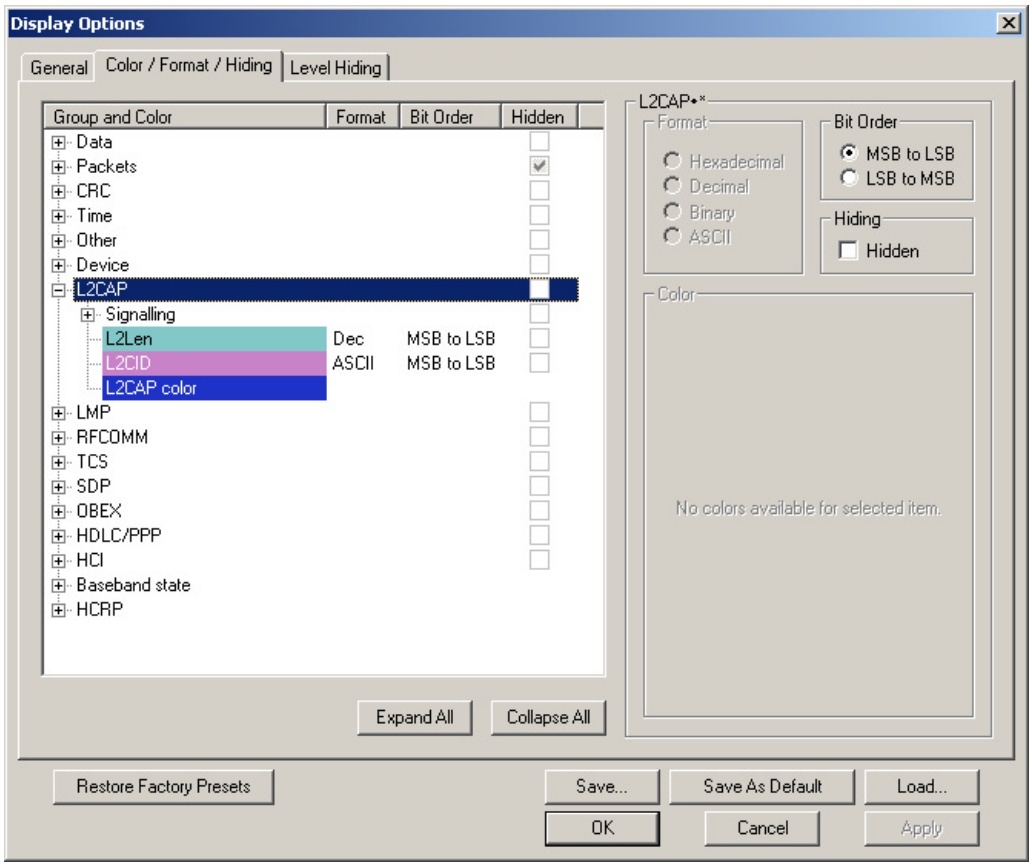
Step 2 Click **Save**...

Step 3 Specify a filename (***.opt**).

Step 4 Click **Save**.

7.2 Setting Color, Formatting, and Hiding Options

Click the **Color/Format/Hiding** tab on the Display Options screen.



Use this window to customize the colors and formats associated with each field in the Trace view. You can also use this window to hide fields within the trace.

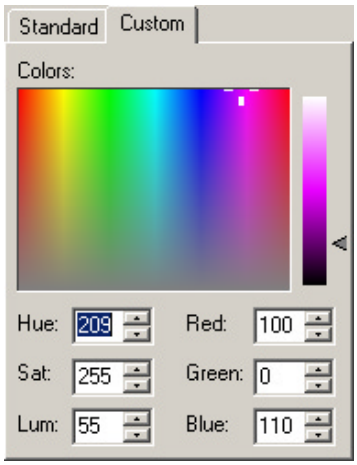
Setting Color Display Options

To change the colors of elements in the trace, select an item in the Group and Color column and use the color pallet screen on the right to make the desired changes.

Note The color of an Invalid Data (packet error) field cannot be changed; it is permanently set to red.

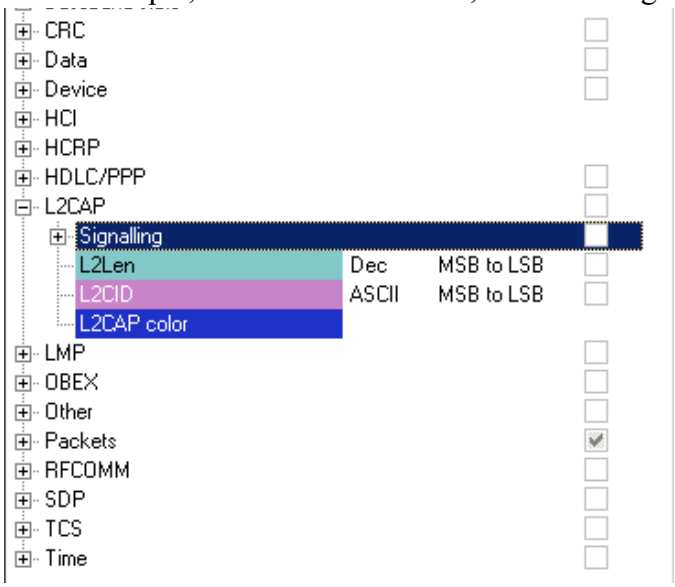
Use this window to customize the colors associated with each field in the trace. You can experiment with these options to achieve the color combination best suited to a particular graphic system.

You can also customize the colors by using the options in the Custom tab.

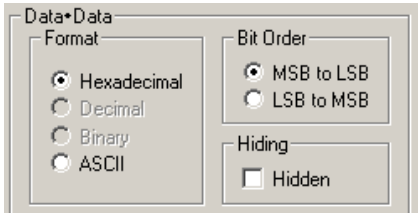


Changing Field Formats

To change field formats, select an item under the Group and Color column. This action will enable the formats radio buttons on the right. The format types change with respect to the item selected under the Group and Color column. For example, if L2CAP is selected, the following displays:



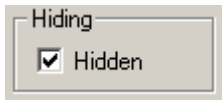
The following formats are available:



Note Not every format is available for every item.

Hiding Display Options

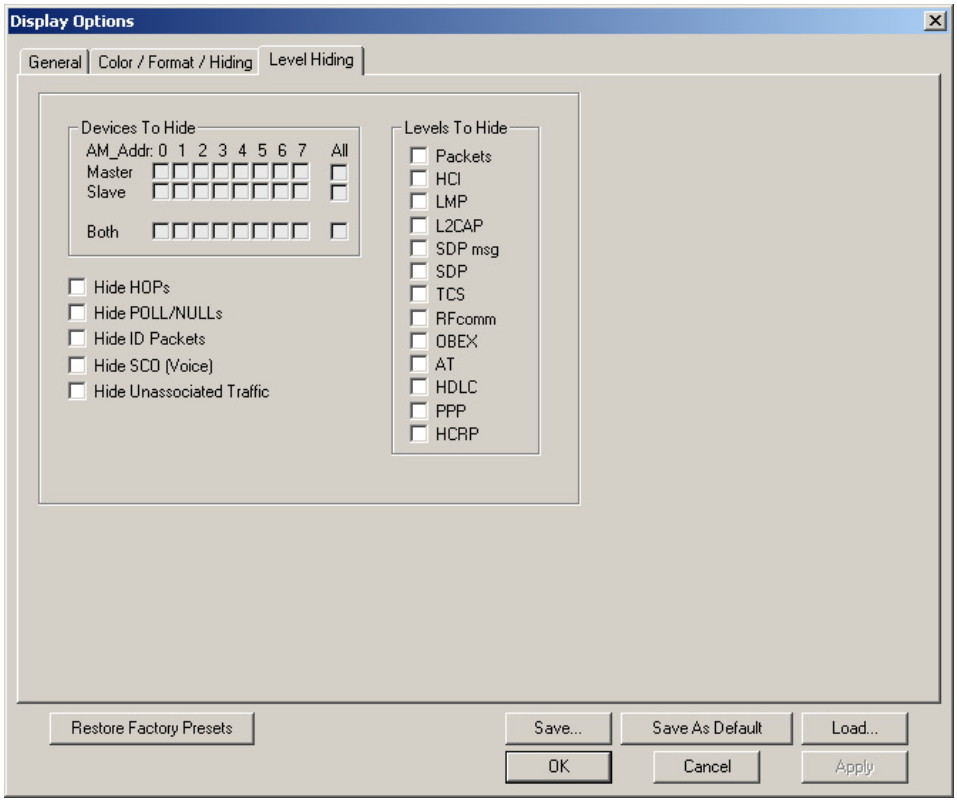
To hide one or more fields in the trace, select the appropriate item from the Group and color column, click the checkbox marked **Hidden**, and click the **Save** button.



You can also hide Sequences from a trace by selecting the desired options from the checkboxes.

7.3 Level Hiding Options

The Level Hiding tab allows you to hide FISs, Idle Sequences and other types of traffic. To hide traffic, select one or more items, then click **Save**.



Level Hiding Parameters

Use the Hiding window to hide various fields, packets, messages, and protocols from the Trace View screen. You can modify these settings at will to display a specific area of a Trace.

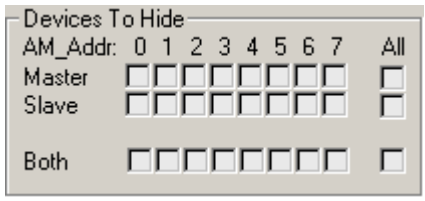
Hiding Fields

The "Hide Fields" checkboxes allow individual fields to be hidden within a trace. Click the checkbox(es) of your choice to hide one or more fields.

Hiding Packets, Messages, and Protocols

The "Hide Packets and Transactions" box contains two grids of checkboxes for hiding whole packets, messages, protocols, and traffic from individual devices. The grids are labeled "Devices to Hide" and "Levels to Hide".

Devices to Hide



The "Devices to Hide" grid lets you hide traffic according to device address. The grid divides into columns which represent different devices.

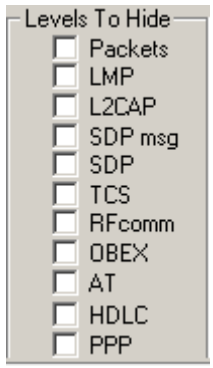
Columns labeled "**0**" through "**7**" and "**All**" represent the **Active Member Address** of a device. By checking one of the boxes in a column, you hide the traffic of the selected device (or traffic from all devices if you have selected **All**.)

The row in which you place your checkmark determines whether you are hiding traffic going to or from a device.

- Master - Hide traffic from a Master to selected Slaves
- Slave - Hide traffic from selected Slaves to the Master
- Both - Hide all traffic between the Master and selected Slave

Example: to hide all traffic from a Master *to* a Slave device with an address of six, click the checkbox under column **6** on the row marked **Master**.

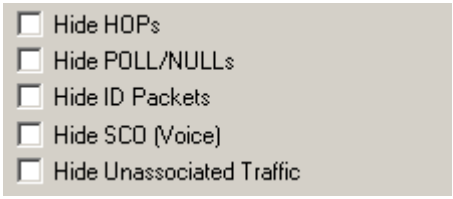
Levels to Hide



The "Levels to Hide" grid divides into rows which represent the different packet, message, and protocol levels. Clicking a checkbox will cause the analyzer to hide all traffic of a selected level.

Hiding Packets

At the bottom of the Hiding tab of the Display Options window, check boxes are available for hiding HOPs, POLLs, NULLs, and other kinds of traffic.

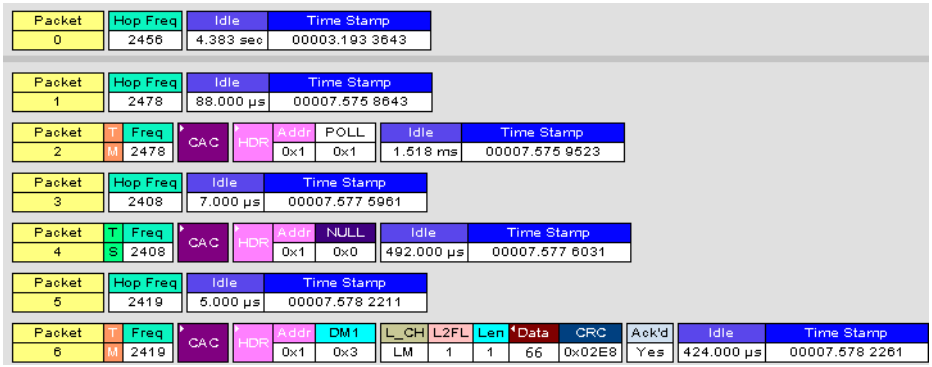


7.4 Saving Display Options

To complete your display options settings, use the features at the bottom of the **Display Options** window. These features remain the same no matter which of the four **Display Options** windows you are working in.

- Click **Save** to save the currently specified display options for use in future sessions. Any file name can be specified, but you must use the **.opt** extension. If no extension is specified, **.opt** is added by default.
- Click **Load** to load a previously saved ***.opt** file, thus restoring a previous set of display options.
- The **Save as Default** function is equivalent to the **Save** function, specifying the file name **default.opt.** Whenever you start up the Analyzer, it automatically loads the **default.opt** file if one exists.
- Click **OK** to apply any changes you have made to **Display Options** and close this dialog box.
- Click **Cancel** to cancel any immediate changes you have made and exit the **Display Options** menu.
- Click **Apply** to apply your changes while keeping the **Display Options** window open.

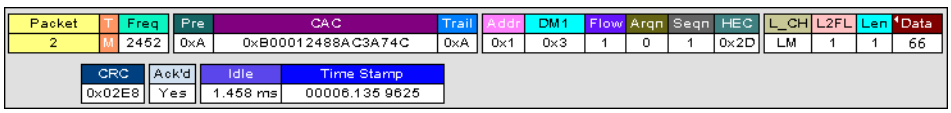
8. Reading a CATC Trace


Packet 0 Hop Freq 2456 Idle 4.383 sec Time Stamp 00003.193 3643
Packet 1 Hop Freq 2478 Idle 88.000 µs Time Stamp 00007.575 8643
Packet 2 T/M Freq 2478 CAC HDR Addr 0x1 POLL 0x1 Idle 1.518 ms Time Stamp 00007.575 9523
Packet 3 Hop Freq 2408 Idle 7.000 µs Time Stamp 00007.577 5961
Packet 4 T/S Freq 2408 CAC HDR Addr 0x1 NULL 0x0 Idle 492.000 µs Time Stamp 00007.577 6031
Packet 5 Hop Freq 2419 Idle 5.000 µs Time Stamp 00007.578 2211
Packet 6 T/M Freq 2419 CAC HDR Addr 0x1 DM1 0x3 L_CH LM L2FL 1 Len 1 Data 66 CRC 0x02E8 Ack'd Yes Idle 424.000 µs Time Stamp 00007.578 2261

8.1 Trace View Features

- The Merlin Mobile packet view display makes extensive use of color and graphics to fully document the captured traffic.
- Packets are shown on separate rows, with their individual fields both labeled and color coded.
- Packets are numbered (sequentially, as recorded), time-stamped, and highlighted to show the device status (master or slave).
- Display formats can be named and saved for later use.
- Pop-up Tool Tips annotate packet fields with detailed information about their contents.
- Data fields can be collapsed to occupy minimal space in the display (which can in turn be zoomed in and out to optimize screen utilization).
- The display software can operate independent of the hardware and so can function as a stand-alone Trace Viewer that may be freely distributed.

8.2 Interpreting the Displayed Information


Packet 2 T/M Freq 2452 Pre 0xA CAC 0xB00012488AC3A74C Trail 0xA Addr 0x1 DM1 0x3 Flow 1 Arqn 0 Seqn 1 HEC 0x2D L_CH LM L2FL 1 Len 1 Data 66
CRC 0x02E8 Ack'd Yes Idle 1.458 ms Time Stamp 00006.135 9625

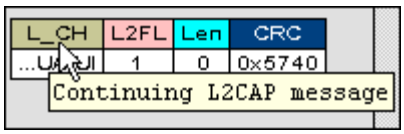
The following table describes the abbreviations used in the Merlin display. Packet #0 is described from left to right:

Packet:#	**Packet/Event Number**
T/M, T/S	M =Master Device Transmitting S = Slave Device Transmitting
Freq	Current Hop Frequency (in MHz)
Pre	Preamble of the Sync word

Packet:#	Packet/Event Number
CAC	Channel Access Code
Trail	Access Code Trailer of the Sync word
Addr	Active Member Address
DM1	DM1 Packet Type
Flow	ACL Link Flow Control
Arqn	Acknowledgment Indication Flag
Seqn	Sequential Numbering
HEC	Header Error Correction Code
L_CH	LMP Message
L2FL	L2CAP Flow Control Flag
Len	Message Length in Bytes including Opcode
TID	LMP Transition initiated by Master
Opcode	LMP-host_connection_req
CRC	Cyclic Redundancy Check
Ack'd	Packet Acknowledgment based on subsequent packet's ARQN with same AM_ADDR
Idle	Idle Time in nanoseconds
Time Stamp	Decimal in Seconds.Milliseconds.Microseconds*10 This is the analyzer internal clock as a reference with resolution of 100 ns.

8.3 Tooltips

You can get additional information about each field in a trace by holding your mouse pointer over a field. A tooltip will appear with details about the field.



8.4 Set Marker

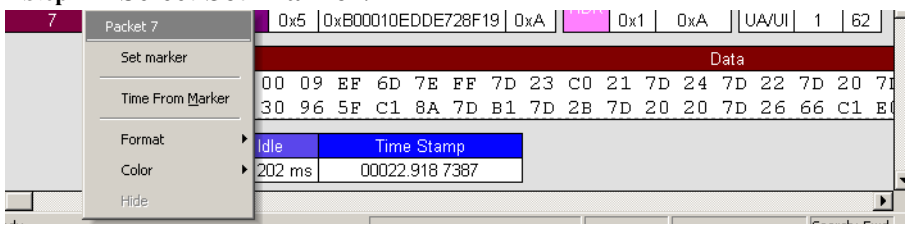
Note **Set Marker** works in conjunction with the **Go to Marker** feature.

You can define a unique Marker for each packet.

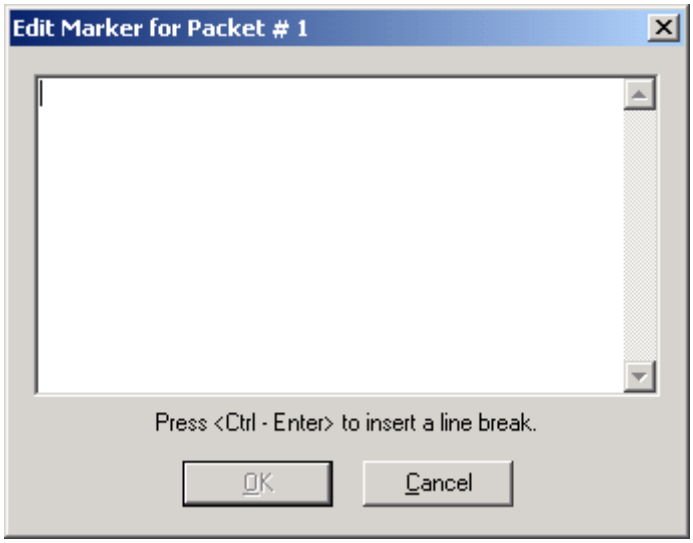
To place a marker on a packet,

Step 1 Left-click on **Packet #** for the packet you wish to mark.

Step 2 Select **Set Marker**.



You see the **Edit Marker Comment** window where you can enter a unique comment about this packet.:



Step 3 Enter your comment.

Step 4 Click **OK**.

A marked packet is indicated by a vertical red bar along the left edge of the packet # block:

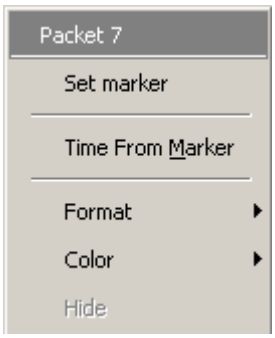
Packet #	T	Freq	Pre	CAC	Trail	Addr	NULL	Flow	Arqn	Seqn	HEC	Time Stamp
1661	S	13	0x5	0xB00010EDDE728F19	0xA	0x1	0x0	1	1	1	0x0B	00060.128 5315

8.5 Edit or Clear Marker

To clear or edit the comments associated with a packet marker,

Step 1 Left-click on **Packet #** for the chosen packet.

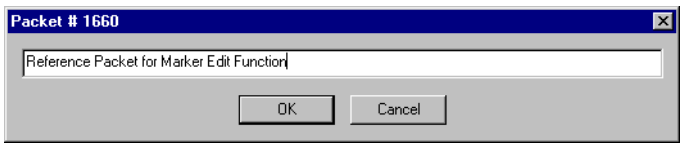
You see the **Packet** menu:



To edit the Marker Comment,

Step 2 Select **Edit marker**.

You see the **Edit marker comment** window:



Step 3 Edit the comment as desired.

Step 4 Click **OK**.

To clear a Marker,

Step 5 Click **Clear marker**.

The vertical red Marker bar disappears.

8.6 Expanded and Collapsed Data Formats

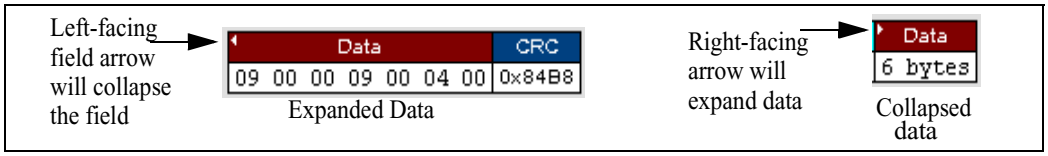
The data field can be expanded to display greater detail or collapsed to a compact view. The Expand/Collapse Data feature operates as a toggle. There are three ways to toggle between the two views.

Double-Clicking

You can expand or collapse a Data field by double-clicking anywhere in the Data field of a packet.

Left-clicking a Field Arrow

Many fields have small arrows in the top left corner. If you left-click this arrow, the field will toggle back and forth between collapsed and expanded views.



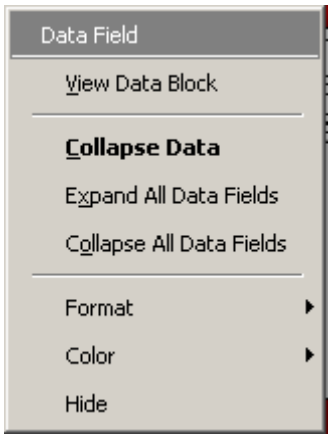
If you click and hold down the left mouse button on one of these arrows, you can collapse or expand the field for *ALL* packets, messages or protocols.

Using the Shortcut Menu

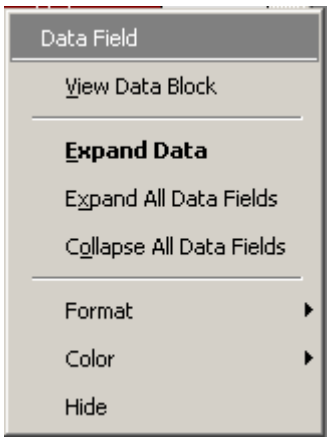
If you left-click on a **Data** field, a menu will open for expanding or collapsing data fields.

Step 1 Left-click on **Data** in the Data packet you want to expand or collapse.

If your Data Trace View is currently expanded, you see the **Collapse Data** menu:



If your Data Trace View is currently collapsed, you see the **Expand Data** menu:



Note that you can choose to expand or collapse

- **Only** the Data in the selected Data packet

  OR

- **All** Data Fields in the Trace View.

Step 2 Select the desired Expand Data or Collapse Data menu item.

The Trace View is repositioned with the selected packet(s) adjusted in the format you have specified.

8.7 Hide Frequency Hops

You can hide Frequency Hops (Hops) from a trace by pressing the **Hide Hops** button on the Tool Bar:

From the Tool Bar

- Click

to hide all Hop packets.

8.8 Hide Nulls and Polls

You can hide Nulls and Polls from a trace by pressing the **Hide Nulls and Polls** button on the Tool Bar.

From the Tool Bar

- Click

to hide all Nulls and Polls.

8.9 Hide ID Packets

You can hide ID packets from a trace by pressing the **Hide ID Packets** button on the Tool Bar.

From the Tool Bar

- Click to hide all ID Packets.

8.10 Hide Voice (SCO) Packets

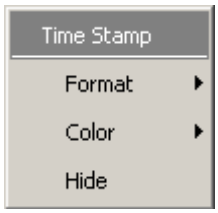
You can hide SCO packets from a trace by pressing the **Hide Voice (SCO) Packets** button on the Tool Bar.

From the Tool Bar

- Click to hide all Voice (SCO) Packets.

8.11 Menus in Clicked Fields

You can display the following menu when you click in a field in a trace.



8.12 Hide Unassociated Traffic

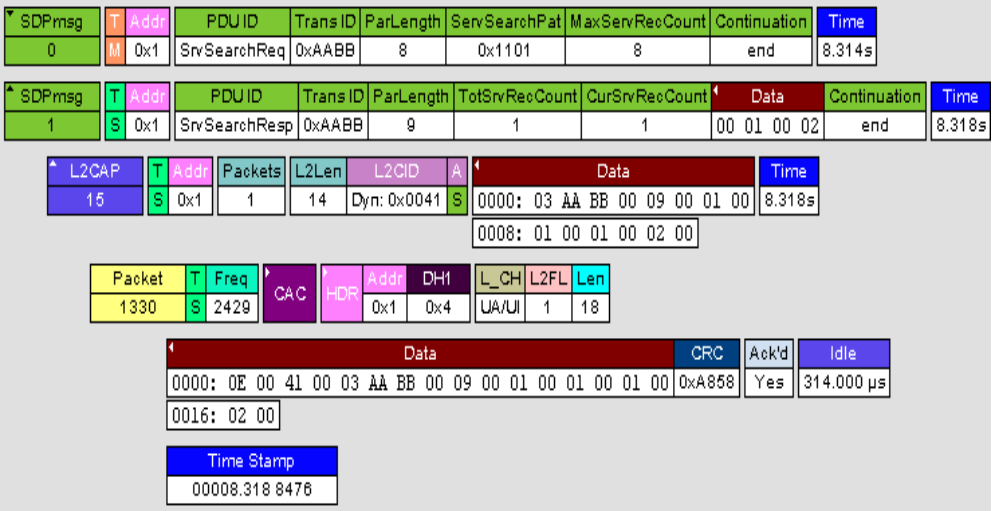
You can hide all traffic that is not associated with the current decode level by pressing the **Hide Unassociated Traffic** button on the Tool Bar.

From the Tool Bar

- First, click one or more decode buttons such as the **View L2CAP Messages** . This button will cause Merlin Mobile to decode the trace and display selected level of decode.
- Next, click to hide all unassociated traffic.

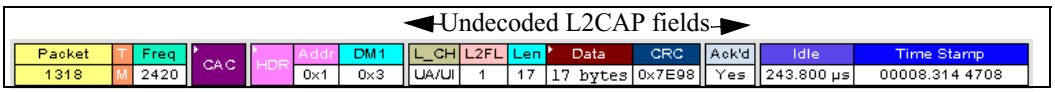
The **Hide Unassociated Traffic** button will cause Merlin Mobile to hide all traffic except for the selected decode messages or protocols. In the example above, all packets would be hidden and only L2CAP messages would display.

9. Decoding Protocols



9.1 Introduction

Merlin Mobile can decode HCI, LMP and L2CAP protocol messages, and RFCOMM, SDP, TCS, HDLC, PPP, OBEX, HCRP, BNEP, HID, IP, TCP, and UDP protocols. The default is *packet level* decoding, which means that baseband packets will be displayed when you first view a trace. If these packets are carrying LMP, L2CAP or higher protocols, the protocols will display as undecoded fields such as the L2CAP packet below.

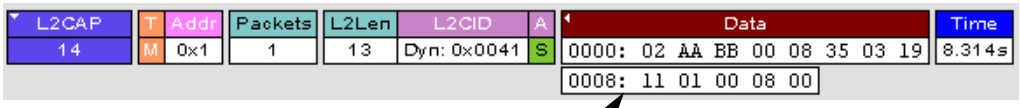


By issuing a decode command, Merlin Mobile can decode these LMP and other fields and display the data in summary statements called *LMP/L2CAP Messages*, *Protocols Messages, and Protocol Transactions*.

9.2 LMP and L2CAP Messages

LMP and L2CAP Messages are lines in a trace that summarize LMP and L2CAP actions such as an *LMP connection request.* LMP and L2CAP Messages summarize the type of action, the number of packets involved in

the action, and the device performing the action. If the message is carrying higher protocol data such as RFCOMM, TCS, OBEX or SDP data, the message displays this data in an undecoded format that can be decoded later.



Undecoded higher protocol data

9.3 Decoding and Viewing Protocol Data

Higher protocol data can be decoded two ways: by clicking a decode button on the toolbar or by selecting a decode command from a pull down menu.

Decoding Via the Decoding Toolbar

The Decoding Toolbar has ten buttons for decoding packets, messages, and protocols:

- **Pkt** (Display Packets)
- **HCI** (Display HCI Protocol)
- **LMP** (Display LMP Messages)
- **L2CAP** (Display L2CAP **M**essages)
- **SDP Msg** (Display SDP Protocol Messages)
- **SDP** Tra (Display SDP Transactions)
- **TCS** (Display TCS Protocol messages)
- **RFCOMM** (Display RFCOMM Protocol)
- **OBEX** (Display OBEX Protocol)
- **AT** (Display AT Commands Protocol)
- **HDLC** (Display HDLC Protocol)
- **PPP** (Display PPP)
- **HCRP** (Display HCRP)
- **AVCTP** (Display AVCTP)
- **AVDTP** (Display AVDTP)
- **BNEP** (Display Bluetooth Network Encapsulation Protocol)
- **HID** (Display HID Protocol)

- **IP** (Display IP)
- **TCP** (Display TCP)
- **UDP** (Display UDP)

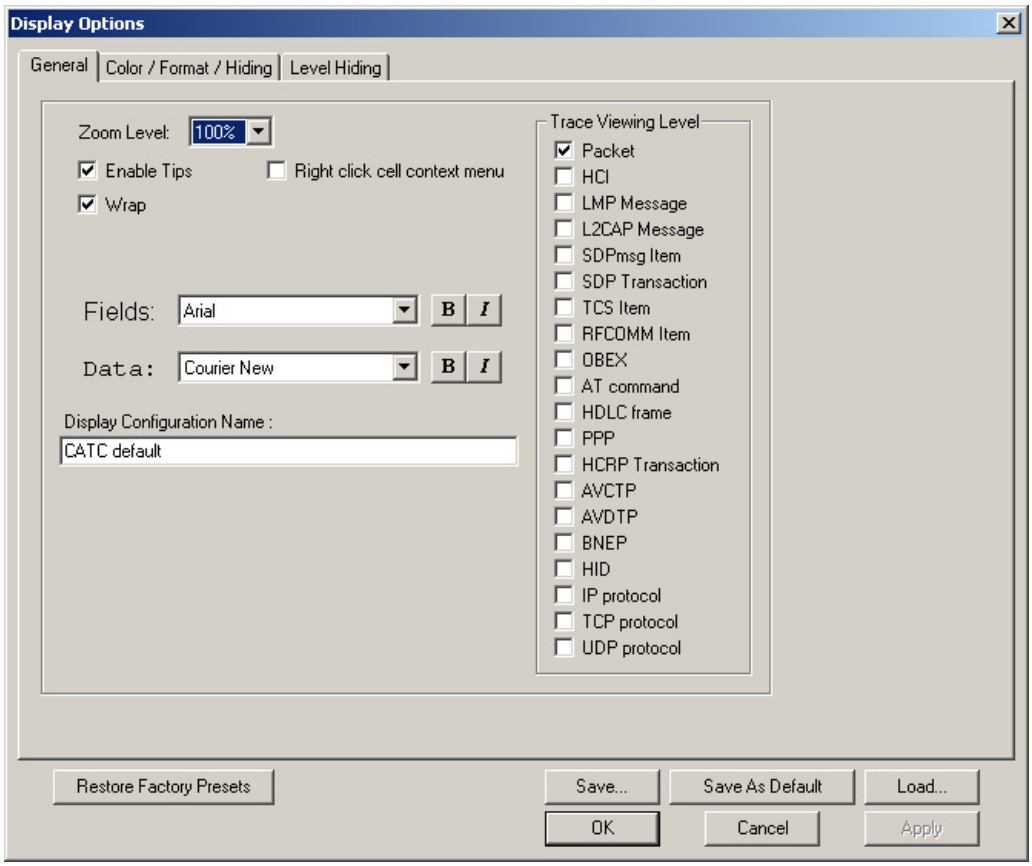
For example, to display LMP messages, click LMP.

Note Once a decode has been performed, it will probably be necessary to scroll through the display to find the decoded messages or protocols. You can shorten your search by first clicking the Hide Unassociated Traffic button .

Decoding Via the Display Options Dialog Box

The Display Options dialog box has three options for issuing decode commands. To issue a command,

Step 1 From the menu bar, select **Setup>Decoding Options**

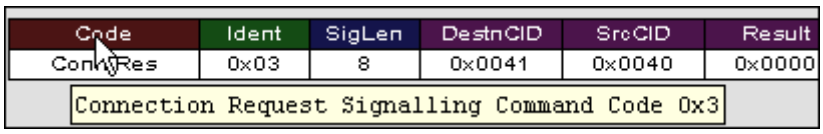


Step 2 Select the option for the desired level of decoding.

Step 3 Click **OK** or **Apply**.

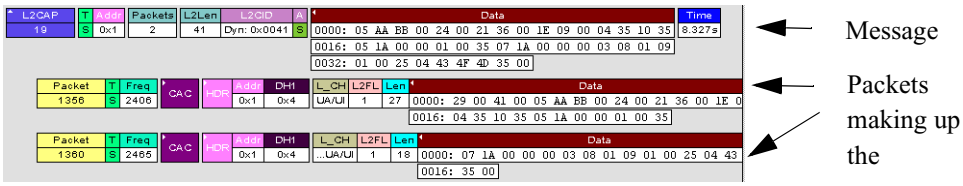
9.4 Tooltips

Additional information about fields can be attained by positioning your mouse pointer over a field of interest. A tooltip will appear that will provide details about the field. In some cases, there can be a considerable amount of information available.



9.5 Viewing Packets in LMP and L2CAP Messages

LMP and L2CAP Messages can be "opened" to reveal their constituent packets by double-clicking the first cell in of the message or clicking once on the small arrow on that same cell. The packets will then display below the message. The following screenshot shows an example of a message and its packets.



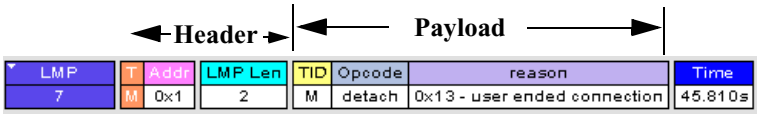
9.6 Types of LMP and L2CAP Messages

If you scroll through a trace, you will see three kinds of message:

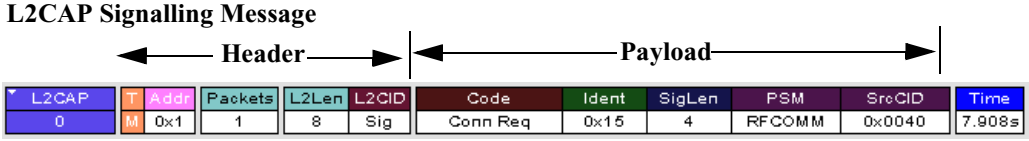
- LMP Signalling Message
- L2CAP Signalling Message
- L2CAP Data Transfer Message

Each message has the same basic message header but differs in its payload.

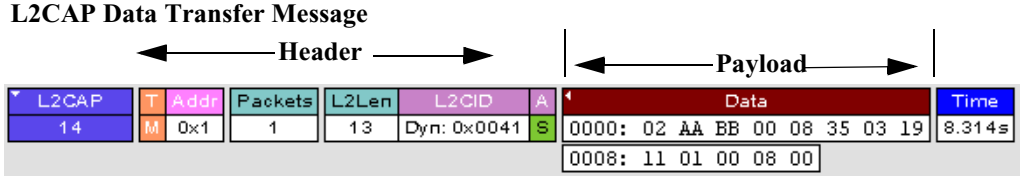
LMP Signalling Message



L2CAP Signalling Message



L2CAP Data Transfer Message



LMP and L2CAP Signalling messages have payloads of commands for establishing LMP and L2CAP channels. L2CAP Data-Transfer messages have a payload that may include RFCOMM, SDP, or TCS data. In order to view higher protocol data, you will need to decode the messages (shown in the next section). The decoded data will appear as new lines in the trace called "Protocol Messages."

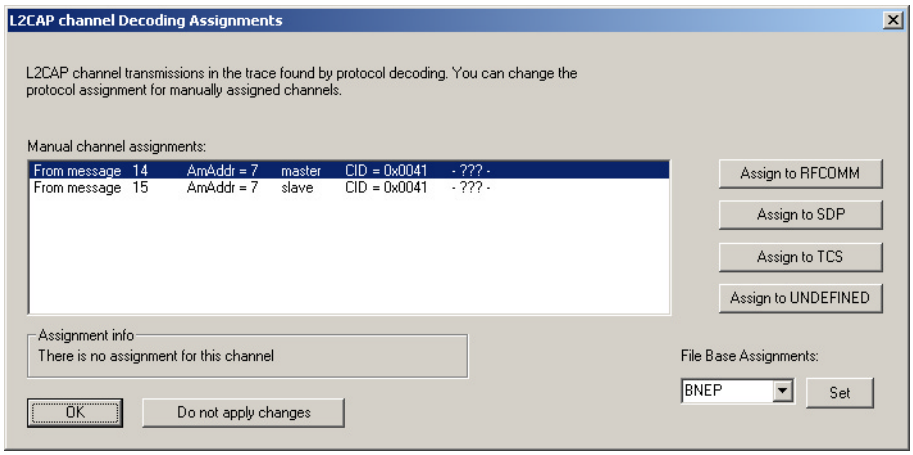
9.7 Viewing L2CAP Channel Connections

Once L2CAP messages have been decoded and displayed, you can check or change their L2CAP channel connections by opening the L2CAP Decoding Connections dialog box.

To view or change an L2CAP channel connection,

Step 1 Select from the menu bar
View>Decoding Assignments

The following dialog box will open.


L2CAP channel Decoding Assignments
L2CAP channel transmissions in the trace found by protocol decoding. You can change the protocol assignment for manually assigned channels.
Manual channel assignments:
From message 14 AmAddr = 7 master CID = 0x0041 - ??? -
From message 15 AmAddr = 7 slave CID = 0x0041 - ??? -
Assign to RFCOMM
Assign to SDP
Assign to TCS
Assign to UNDEFINED
Assignment info
There is no assignment for this channel
File Base Assignments:
BNEP
Set
OK
Do not apply changes

Step 2 Click on a channel assignment and then look at the Connect and Disconnect buttons on the far right of the dialog box.

If the Connect and Disconnect buttons are grayed-out, it means that Merlin Mobile made the channel assignments using data in the trace. You can verify that Merlin Mobile performed the assignments by looking at the text in the "Slave Channel" box in the lower left corner of the dialog box. If you see "Connection Recorded" it means that Merlin Mobile performed the channel assignments.

If Merlin Mobile was not able to make these channel assignments, then the Connect and Disconnect buttons on the right side of the dialog box will be active. You can then assign and edit channel connections.

Step 3 Open the drop-down menu labeled AM_Addr (Active Member Address). If possible, select an address other than the currently displayed address.

The connections for the 'new' device should now display.

9.8 Viewing Protocol Messages and Transactions

By pressing a button such as SDP Msg or OBEX, you can cause Merlin Mobile to decode the higher level protocol data contained within L2CAP messages and display them as packet-like rows called *Protocol Messages*. Protocol Messages have headers marked "protocol" and fields that vary in appearance and content depending on the type of protocol.

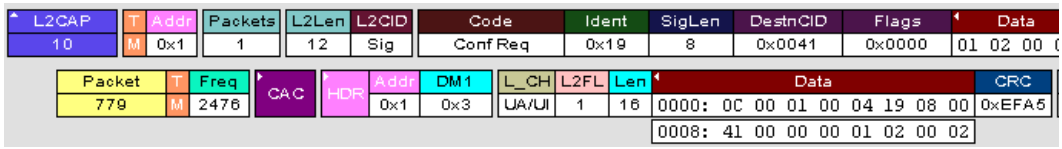
Some Protocol Messages can be grouped into a higher level entity called a *Protocol Transaction*. A Protocol Transaction is a row in a trace that summarizes the higher level protocol data that is transmitted between a Master and Slave device when one sends a request and the other sends back

a response. For example, if you press

, Merlin Mobile will locate SDP requests and responses between a Master and Slave device summarize their data.

Viewing L2CAP Messages in Protocol Messages

If the protocol heading is double-clicked, the L2CAP data-transfer messages that make up the protocol will display below the protocol. You can also expand the protocol by left-clicking the small downward pointing arrow on the protocol header.



How to Decode

Decoding Protocol messages is the same process as decoding LMP and L2CAP messages.

Using the Toolbar - To decode using the Toolbar, press one of the protocol decode buttons such as:

.

Using the Menu - To decode using the menu, select:
Setup>Display Options

Then select one of the decode checkboxes.

Once a decode command has been issued, Merlin Mobile will create Protocol Messages in the trace. You will probably have to hide hops, polls, and null packets and then scroll through the trace in order to find Protocol messages.

Expanding Protocol Messages

Protocol messages can be expanded to reveal their constituent packets using any of the following methods:

- Left-click the small downward pointing arrow in the message/protocol header

- Double-click a message/protocol header
- Left-click the message/protocol header and choose "Expand Transaction" from the short-cut menu

9.9 Changing Protocol Assignments

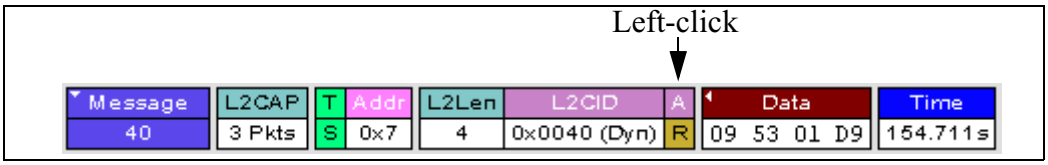
If a sequence of messages is assigned the wrong protocol, errors will display. To change or remove a protocol assignment, you will need to access the **Assignment** menu and issue an Add Assignment command.

Step 1 Click L2CAP to display L2CAP messages.

Note You need to view L2CAP Messages in order to have access to the "**A**" field that permits reassigning protocols.

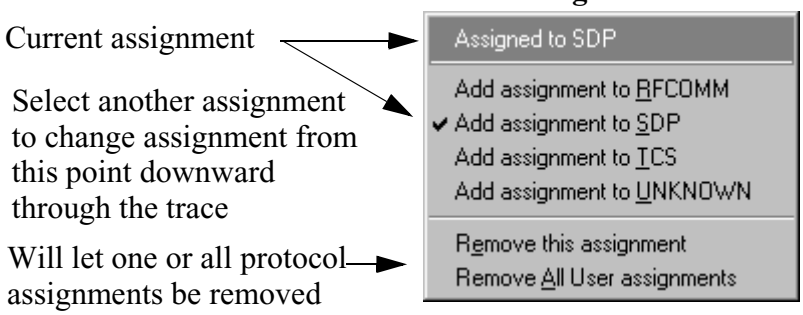
Step 2 Scroll through the trace until you have located an L2CAP message with a field marked "**A**."

Step 3 Left-click the field marked "**A.**"



An **Assignment** menu will open for assigning, re-assigning, or un-assigning protocols to messages. This menu is context-sensitive and will vary in content depending on the protocols in the trace.

The Assignment Menu


Current assignment
Select another assignment to change assignment from this point downward through the trace
Will let one or all protocol assignments be removed
Assigned to SDP
Add assignment to RFCOMM
Add assignment to SDP
Add assignment to TCS
Add assignment to UNKNOWN
Remove this assignment
Remove All User assignments

Step 4 From the menu, select one of the "Add Assignment" options not already selected.

At this point, the protocol assignment will change to your selection.

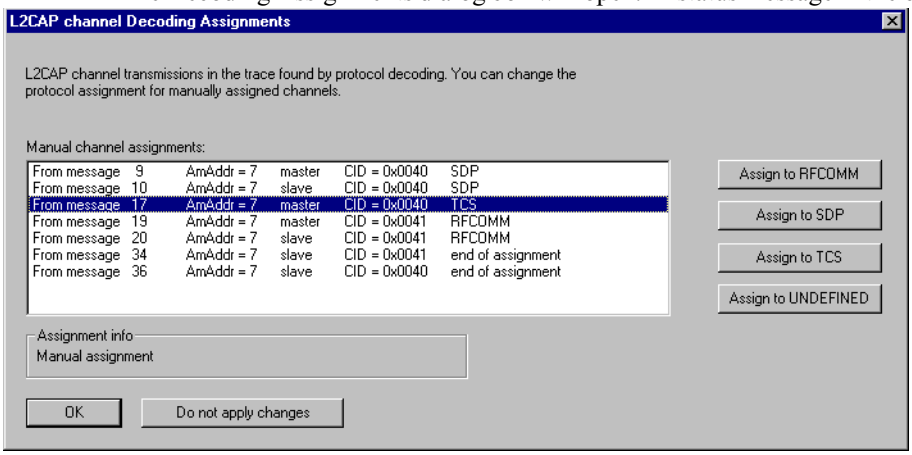
Using the Decoding Assignments Dialog Box

You can get a complete list of all protocol assignments by opening the Decoding Assignments dialog box. This dialog box will tell you which protocol assignments were made by Merlin Mobile and which are user-assigned. User-assigned protocols can be reassigned if need be using this dialog box.

To open the Decoding Assignments dialog box and reassign a protocol,

Step 1 Select from the menu
View>Decoding assignments

The Decoding Assignments dialog box will open. A status message in the bottom


L2CAP channel Decoding Assignments
L2CAP channel transmissions in the trace found by protocol decoding. You can change the protocol assignment for manually assigned channels.
Manual channel assignments:
From message 9 AmAddr = 7 master CID = 0x0040 SDP
From message 10 AmAddr = 7 slave CID = 0x0040 SDP
From message 17 AmAddr = 7 master CID = 0x0040 TCS
From message 19 AmAddr = 7 master CID = 0x0041 RFCOMM
From message 20 AmAddr = 7 slave CID = 0x0041 RFCOMM
From message 34 AmAddr = 7 slave CID = 0x0041 end of assignment
From message 36 AmAddr = 7 slave CID = 0x0040 end of assignment
Assign to RFCOMM
Assign to SDP
Assign to TCS
Assign to UNDEFINED
Assignment info
Manual assignment
OK
Do not apply changes

left corner of the dialog box will indicate who assigned the protocol.

Step 2 Click on one of the displayed assignments.

If the protocol was assigned by Merlin Mobile, the Assign buttons on the right will be grayed out and unavailable. If you want to change these assignments, you will have to use the pop-up menus described in the previous section. If a protocol has been manually assigned by a user, the Assign buttons will become active and allow you to make a change in assignment.

Step 3 If possible, click the appropriate Assign button.

Removing User-Assigned Protocol Assignments

As you practice assigning and reassigning protocols, you will find that one of the more useful commands is "Remove All User Assignments." This command allows you to undo all of your assignments.

To remove some or all user-assigned protocol assignments,

Step 1 Double-click any Protocol Message header to open view L2CAP messages.

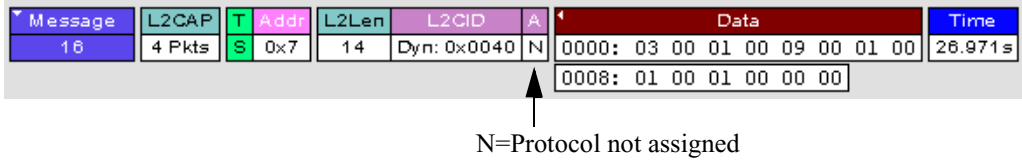
Step 2 Locate a message with a field marked "**A**."

Step 3 Left-click on the "A" field to open the Assignment menu.

Step 4 Select "Remove All User assignments" or "Remove this assignment."

Manually Assigning Protocols

If a recording does not capture the beginning of a dialog between a Master and Slave devices, Merlin Mobile may not have the L2CAP messages it needs to determine the correct protocol assignments. In this case, L2CAP messages will display an "N" in the Assignment field that means "Not Assigned."



An L2CAP message without a protocol assignment for the higher protocol data.

If you know what the protocol assignment should be for the missing assignments, you can manually add them by right-clicking your mouse over the A field shown above and selecting from the pop-up Assignment menu shown on the previous page.

Other Assignments: OBEX Client/Server Status

OBEX messages carry a status that indicates whether the transmitting device is an OBEX client or OBEX server.

To view an OBEX message's client/server status,

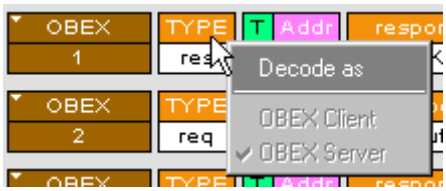
Step 1 Open an OBEX trace file such as the sample file "OBEXsample.tfb" in C:\Program files\CATC\Merlin Mobile.

Step 2 Press . , and to hide Hops, NAKs, and unassociated traffic.

Step 3 Press to decode OBEX.

Step 4 Left-click your mouse over the field marked Type.

A pop-up menu will appear indicating whether the message was produced by an OBEX client or server. If the menu items appear grayed-out (as they do in this



Left-click over the Type field to open the OBEX Client/Server Assign menu.

example) it means that Merlin Mobile assigned the client or server status based on data it found in the trace. If the menu items appear in black, it means that the user assigned the status and is therefore free to change the assignment.

Changing an OBEX Client or Server Status

If the beginning sequence of traffic is not recorded in a trace, the client/server status of the transmitting devices will not be preserved in the trace. In this case, the OBEX Client/Server pop-up menu will become active and you will be able to change the assignment.

Decoding BNEP

BNEP (Bluetooth Network Encapsulation Protocol) is a protocol that allows devices to encapsulate network protocols such as IP. Since BNEP can carry different types of network protocols, you need to tell Merlin Mobile what protocol the BNEP is going to be carrying. You do this via a script file called *bnep.dec* that is read during the initialization of the Merlin Mobile software. This file tells Merlin Mobile how to decode BNEP fields. Once read, BNEP can be correctly decoded by pressing the BN EP button on the toolbar. If the decode file is not read at initialization, Merlin Mobile will display the data in an undecoded format.

For more information on BNEP decoding, see a supplemental document on BNEP in the support directory on the CATC web site:

http://www.catc.com/products/support/sup_Merlin Mobilebluetooth.html

Decoding HID

HID (Human Interface Device) is a profile associated with traffic from devices such as a mouse or a keyboard. To decode HID traffic, you will need to tell Merlin Mobile what types of HID traffic it will be recording. You do this by editing a script file called *hid.dec*. Merlin Mobile reads this file during the initialization of the Merlin Mobile software. This file tells Merlin Mobile how to decode the HID fields. Once read, HID can be correctly decoded by pressing the HID button. If the decode file is not read at initialization, Merlin Mobile will display the data in an undecoded format.

Other Decoding Options

Other decoding options include the following:

- IP
- TCP
- UDP
- AVCTP
- AVDTP
- HCRP

10. Other Features

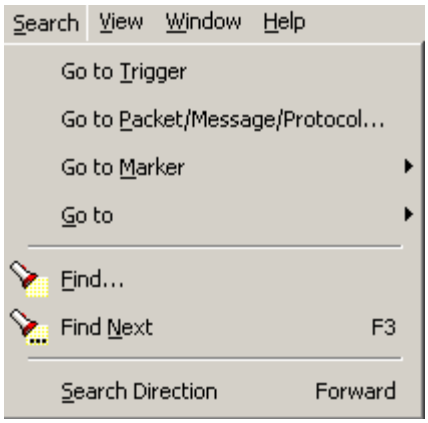
10.1 Search

The Search feature provides several options for searching through recorded traffic, allowing you to find specific packets based on triggering status, packet number, marking, or content.

To view the Search options,

- Click **Search** in the Menu bar.

  You see the Search drop-down menu:



Go to Trigger

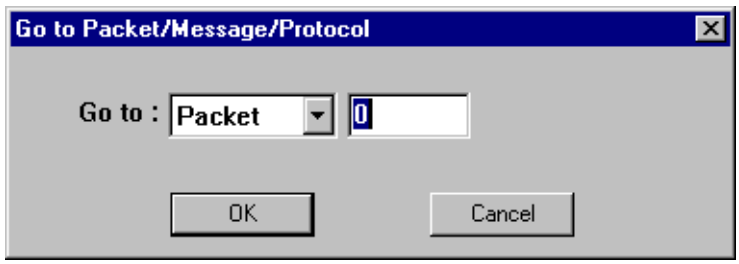
To display a triggering event, select **Go to Trigger** under **Search** on the Menu bar. The **Trace Viewer** display will reposition the trace to show the triggering event at the top of the screen.

Go to Packet/Message/Protocol

To display a specific packet, Message or Protocol

Step 1 Select **Go to Packet/Message/Protocol** under **Search** on the Menu Bar.

You see the **Go to Packet/Message/Protocol** window:



Step 2 Enter the number of the packet, message or protocol you want to display.

Step 3 Click **OK.**

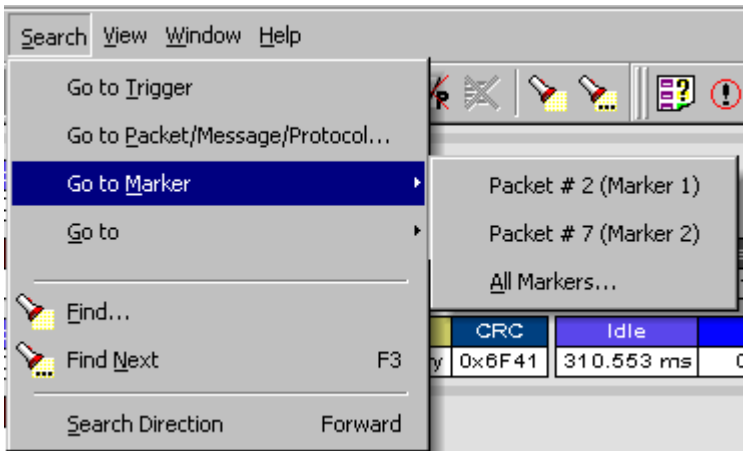
The Trace View repositions to show the packet at the top of your screen.

Go to Marker

To instruct the analyzer to display a marked packet,

Step 1 Select **Go to Marker** under **Search** on the Menu Bar.

You see a drop-down menu listing the marked packets in that Trace View:



Step 2 Select the desired packet from the displayed list.

The Trace View repositions to show the packet at the top of your screen.

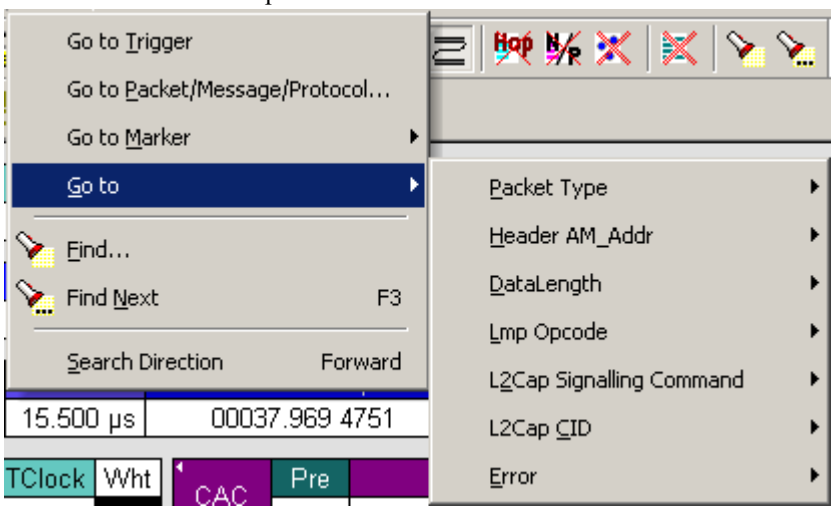
Note The **Go to Marker** feature functions in conjunction with the **Set Marker** feature. The comments within the parentheses following each marked packet are added or edited with the **Set Marker** feature.

Go to

The **Go To** feature takes you directly to an event in a Trace.

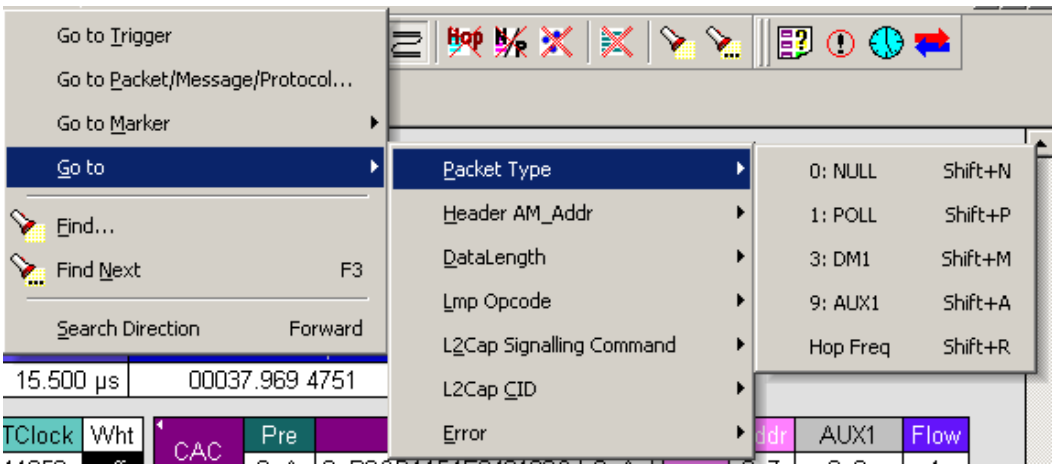
Step 1 Select **Go To** under **Search** on the Menu Bar.

You see the **Go To** drop-down menu:



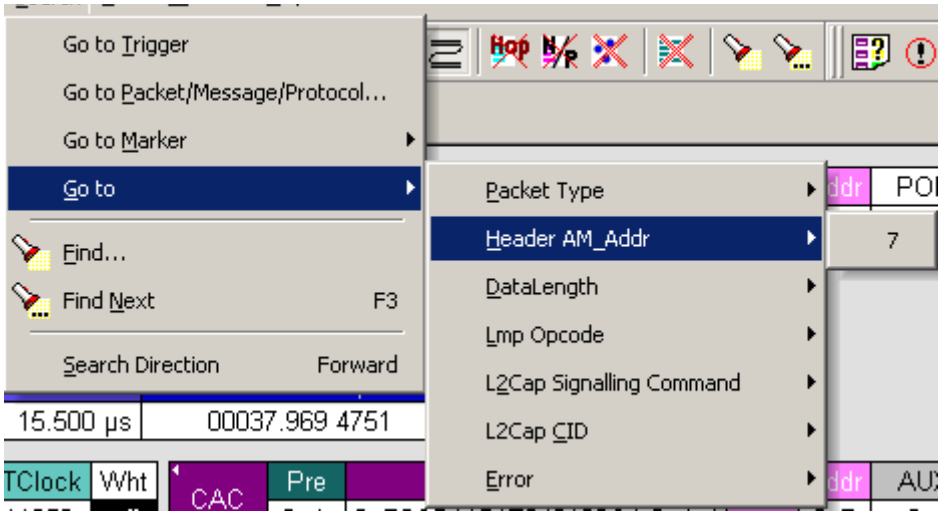
Step 2 Select the event you want to go to and enter the necessary information.

Packet Types



Select the type of packet you want to go to.

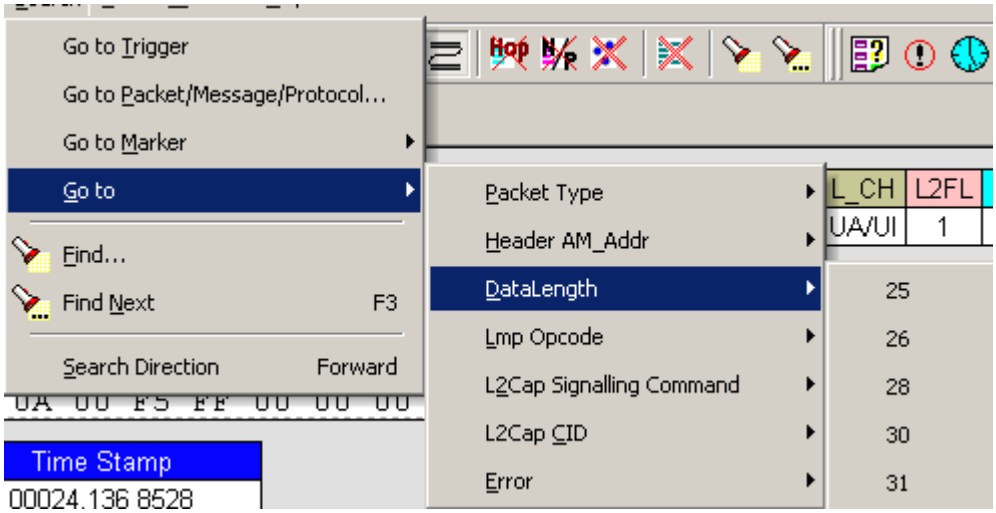
Header AM_Addr



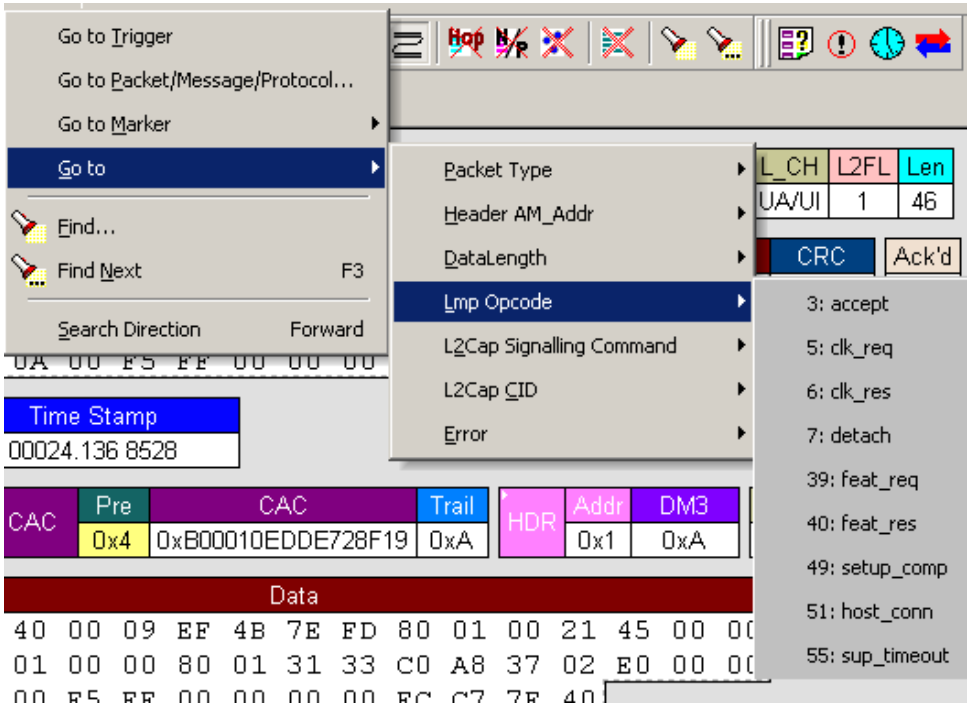
Select an Active Member Address from the list.

DataLength

Allows searching based on data length in bytes from the recording.

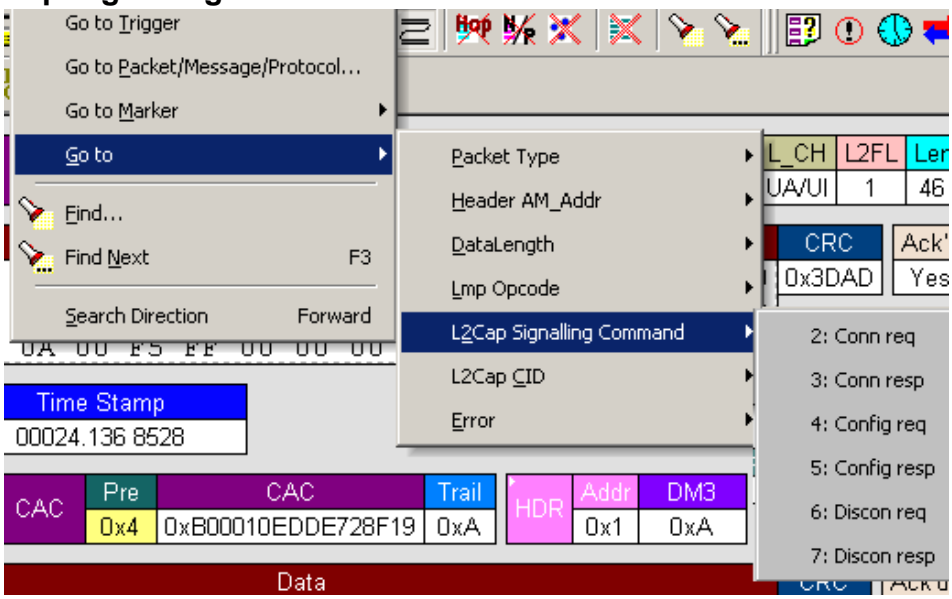


Lmp Opcode



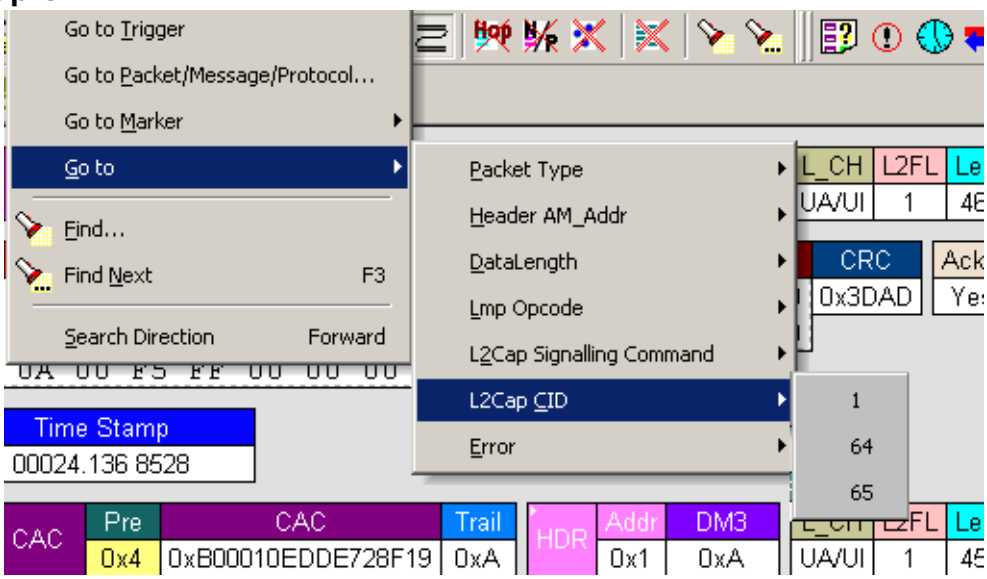
Select the Link Management Protocol Operational Code (Lmp Opcode) that you want to go to.

L2Cap Signalling Command



Select the type of L2Cap Signalling Command that you want to go to.

L2Cap CID



Select the L2Cap Channel ID (L2 Cap CID) that you want to go to.

Error

Moves trace view to next uncorrected error.

Soft Bit Error

Moves trace view to next soft (corrected) error.

Loss of Sync

Moves trace viewer to the next loss of sync.

Find

Find is a utility that allows you to conduct searches of one or more events within a trace. Find allows you to search different hierarchical levels within the trace - packets, LMP Messages, L2CAP messages etc.

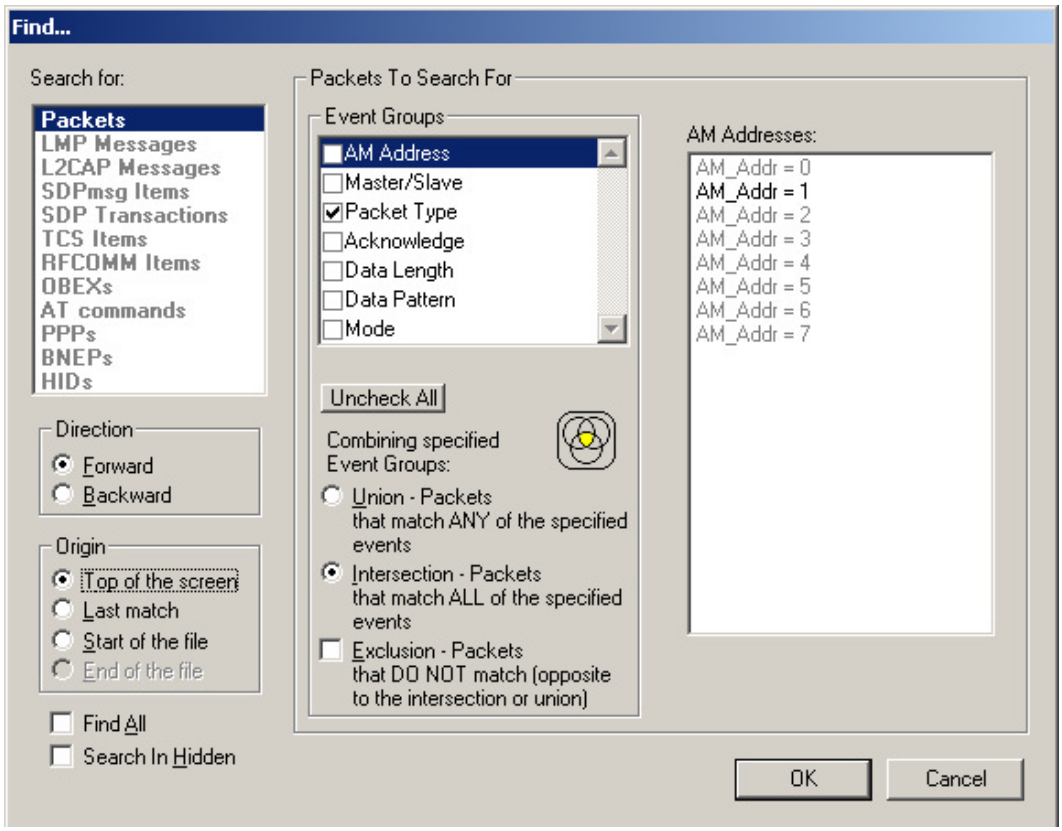
To start find,

- Select **Find...** under **Search** on the Menu Bar

OR

Click in the Tool Bar.

You see the **User-Defined Find Events** screen:



The **Find** window divides into three areas:

Left area -- Controls the search level, search direction and search origin.

Find All - Extracts the results and place them in a separate trace.

Search In Hidden - Searches all packets including packets that have been hidden.

Center area -- Controls the event groups to be searched. The selection you make will display further choices on the right side of the Find window. At the bottom are three options called Union, Intersection, and Exclusion that are used with multi-criteria searches. These options are explained below.

Right area -- Controls the specific events to be searched within the trace. The box in this right section displays events from the selected Event Group.

The right area is context sensitive -- the Event Group selected in the Center area will determine what events will display on the right. For example, if you select **Packet Type**, the Right area will show you a list of packet types. Bold entries in the list represent items that actually occurred in the trace.

In the screenshot shown above, for example, AM Address is selected. On the right, you see that only Address 1 is in bold. This indicates that only a single device was transmitting traffic in the displayed trace.

Event Groups

Event Groups are categories of events that can occur in a trace. Clicking on an Event Group will display a list of Event types on the right side of the Find window that occur within each Event Group.

AM Address

Contains a list of seven Active Member addresses. Bold entries represent devices that occur in the trace.

Master/Slave

Contains two options labeled **Master** and **Slave**. Selecting an option will cause Merlin Mobile to search for traffic based on the selected role.

Packet Type

Contains a list of all Bluetooth packet types. If a packet type occurs in the trace, it will appear in bold.

Acknowledge

Contains a list of three Acknowledge types: **Explicit NAK**, **Implicit NAK**, and **ACK.** The three Acknowledge types are responses a device can issue to attempts to transmit packets to it.

A device can send an Acknowledgment in two ways: through setting the ARQN field to 0 (= explicitly not acknowledged), to 1 (explicitly acknowledged) or by sending an empty packet that does not have an ARQN field (= implicitly not acknowledged).

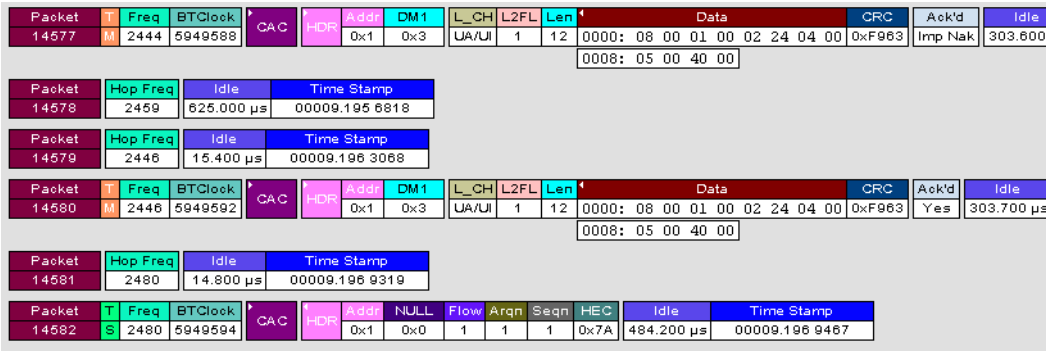
Explicit NAK - Explicitly not acknowledged. An Explicit NAK is an explicit response by a device that it did not receive a data packet. The Explicit NAK is transmitted in the ARQN field (=Acknowledgment Request Negotiation field). ARQN=0 means 'Explicit NAK.'

Implicit NAK - Implicitly not acknowledged. An Implicit NAK is a NAK that is implied rather than explicitly stated. If a device responds to a data packet by sending an empty packet, the NAK is implied.

ACK - Acknowledged. If a data packet is successfully transmitted to a target device, the target device acknowledges the received packet by setting the ARQN field to 1.

Acknowledgments are easily seen in Merlin Mobile traces because Merlin Mobile adds an **Ack'd** field on data packets of the transmitting device. This means that you do not have to hunt through the trace to see if the packet was acknowledged.

The following screenshot shows two examples of Acknowledgments.

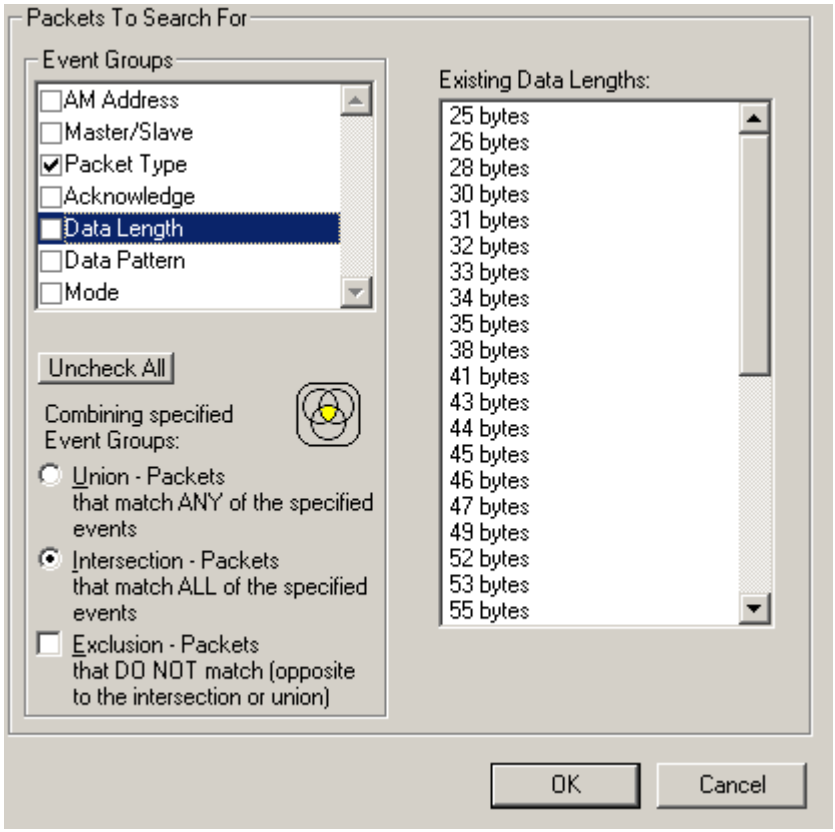

Packet T Freq BTClock CAC HDR Addr DM1 L_CH L2FL Len Data CRC Ack'd Idle
14577 M 2444 5949588 0x1 0x3 UA/UI 1 12 0000: 08 00 01 00 02 24 04 00 0xF963 Imp Nak 303.600
0008: 05 00 40 00
Packet Hop Freq Idle Time Stamp
14578 2459 625.000 µs 00009.195 6818
Packet Hop Freq Idle Time Stamp
14579 2446 15.400 µs 00009.196 3068
Packet T Freq BTClock CAC HDR Addr DM1 L_CH L2FL Len Data CRC Ack'd Idle
14580 M 2446 5949592 0x1 0x3 UA/UI 1 12 0000: 08 00 01 00 02 24 04 00 0xF963 Yes 303.700 µs
0008: 05 00 40 00
Packet Hop Freq Idle Time Stamp
14581 2480 14.800 µs 00009.196 9319
Packet T Freq BTClock CAC HDR Addr NULL Flow Arqn Seqn HEC Idle Time Stamp
14582 S 2480 5949594 0x1 0x0 1 1 1 0x7A 484.200 µs 00009.196 9467

Implicit NAK - Packet 14577 is a data packet sent by the piconet Master device. Packet 14579 should have been a data packet with an acknowledgment. Instead, it is an empty packet. This Master interprets this empty packet as an **Implicit NAK** (i.e., implicitly not acknowledged). Merlin Mobile summarizes this packet exchange by adding an **Ack'd** field to the Master's data packet and setting the **Ack'd** field to **Imp Nak**.

ACK - Packet 14580 is the Master's retransmission of the data sent in packet 14577. Packet 14582 is the reply by the Slave device. This reply contains an ARQN field with a value of (= Acknowledge). Merlin Mobile summarizes this packet exchange by setting the **Ack'd** field on packet 14580 to **Ack**.

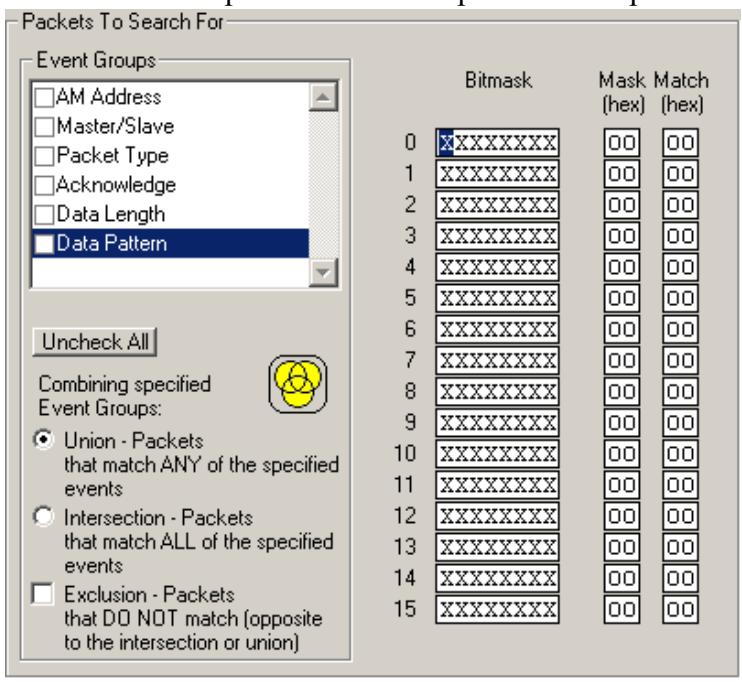
Data Length

Contains a list of all data lengths that occur in the trace.



Data Pattern

Searches for the next packet that has a specified data pattern.



Searching for Bit Patterns

You search for a bit pattern by using the box labeled **Bitmask**. Enter one of the three following values:

- X = 'Don't care,'
- 0 = 'Match a 0',
- 1 = 'Match a 1.'

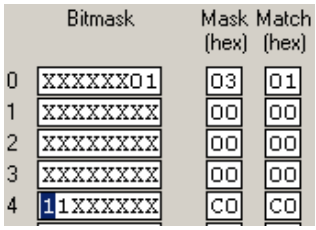
Example -- xxxxxx01 means 'Look for a data pattern where the first 6 bits can be any value but the last two bits must be 01.'

Searching for Long Patterns

You can search for long pattern sequences by entering patterns into multiple rows within the editor. Entering a pattern on one row and skipping several rows before entering the second pattern tells Merlin Mobile to search for the entire pattern between the two specified rows.

Example - Enter xxxxxx01 in row 1 and 11xxxxxx in row 2. This pattern means 'Look for the pattern xxxxxx0111xxxxxx.'

Example - If you enter xxxxxx01 into row 0 and 11xxxxxx into row 4, it means 'Look for the pattern xxxxxx01 xxxxxxxx xxxxxxxx xxxxxxxx 11xxxxxx.'



Searching for Hexadecimal Patterns

The columns marked Match and Mask allow you to specify a pattern in hex. You enter the pattern you want to match in the column marked Match, and enter the mask in the column marked Mask. The Mask column allows you to specify which bits you are searching for.

Example - A Match of 03 and a Mask of '0F' tells Merlin Mobile that you are looking for the hex pattern of 03 occurring in the last four bits of the pattern. If you enter these values in the Match and Mask columns, the Bitmask section will automatically display the equivalent bit values: XXXX0011.

Union, Intersection, and Exclusion

If you select multiple events, you will need to use the options Union or Intersection to conduct the search.

Union is used to search for any selected event: "Find x or y." Union lets you tell the analyzer to search the trace for any of any of the selected items.

Intersection is used to search for all selected events: "Find x and y." Intersection lets you tell the analyzer to search the trace for any packet having all of the selected events.

Exclusion is used to exclude selected traffic from the trace. Exclusion is used with Union and Intersection --i.e., you select Exclusion with Union or Intersection.

- **Exclusion + Union** -- tells Merlin Mobile to exclude packets with any of the specified events.
- **Exclusion + Intersection** -- tells Merlin Mobile to exclude packets with all of the specified events.

Using Find

Step 1 Select the display level to be searched from the **Search For** box on the left side of the window.

For example, to search through L2CAP messages, select L2CAP. The display level that you select will affect options presented in the Events Group box.

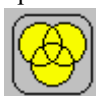
Step 2 Select a search direction and origin.

Step 3 Select one or more events from the **Events Group** box.

Your choices will affect options presented in the box on the right side of the screen.

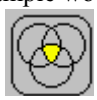
Step 4 If you have selected two or more criteria, then select either :

- **Union:** Find all packets that match ANY of the specified events. An



example would be to find packets with either X or Y.

- **Intersection:** Find all packets that match ALL of the specified events. An example would be to find all packets with X and Y.



If you want to selected events from the trace, then select:

- **Exclusion:** Exclude all packets that match any of the specified events. This option works in conjunction with Union and Intersection. Select an exclusion plus one of the other two options. If you select Exclusion and Union, it means Exclude packets in any of the following events. An example would be to exclude packets with either X or Y.

Step 5 Click **OK**.

The search will then occur. Afterwards, the packets meeting the search criteria will display.

Some Find Examples

Search for all DM1 and Poll packets with an Active Member Address of 7.

Step 1 From the Event Group, select **Packet Types**.

Step 2 From the box on the right, select **DM1** and **Poll**.

Step 3 From the Event Group, select **Header AM_Addr**.

Step 4 From the box on the right, select **AM_Addr=7**.

Step 5 From the Center area, select **Intersection**.

Selecting Intersection tells Merlin Mobile to find packets with ALL of the selected traits.

Step 6 Press **OK**.

The trace should reposition to the first DM1 or Poll packet that has an Active Member address of 7.

Exclude all DM1 and Poll Packets with Active Member Addresses of 7.

Step 1 Select **Packet Types** from the From the Event Group

Step 2 Select **DM1** and **Poll** from the box on the right.

Step 3 Select **Header AM_Addr** from the Event Group.

Step 4 Select **AM_Addr=7** from the box on the right.

Step 5 From the Center area, select **Intersection and Exclusion**

Step 6 Press **OK**.

The trace will redisplay so that it excludes *DM1 packets with AM_Addr=7* and *Poll packets with AM_Addr=7*.

Exclude all packets with ANY of the following attributes: DM1, Poll, or AM_Addr=7.

Step 1 Select **Packet Types** from the Event Groups.

Step 2 Select DM1 and Poll from the box on the right.

Step 3 Select **Header AM_Addr** from Event Group.

Step 4 Select **AM_Addr=7** from the box on the right

Step 5 Select **Union** and **Exclusion**.

Selecting Union causes the analyzer to search for any of the selected events.

Step 6 Press **OK**.

The trace will redisplay so that it excludes *DM1s, Polls, or any packet with AM_Addr=7*.

Find Next

To apply the previous **Find** parameters to the next search,

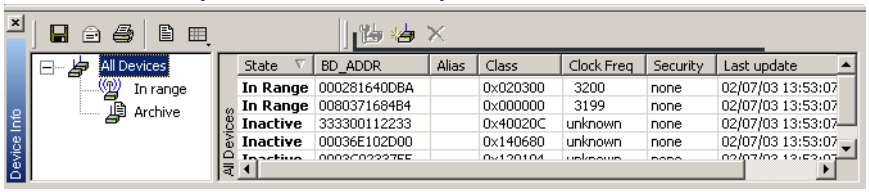
- Select **Find Next** under **Search** on the Menu Bar

  OR

  Click on the Tool Bar.

10.2 Device List

Device List describes devices discovered in a previous inquiry or was entered by the user. The list is stored in a file from one session to the next, so the information one a device that was collected in previous sessions or was manually entered can always be viewed.



By default, Device List appears at the bottom of the Merlin Mobile application window. If is not open, you can open it by selecting **View > Device List**.

Fields in the Device List

- **State** -- Device State
- **BD_ADDR** -- Bluetooth Device Address
- **Alias** -- Whatever alias you entered for the device in the Add New Device dialog
- **Class** -- The device class for each listed device
- **Clock Freq** -- Shows the device's Clock Frequency
- **Security** -- If Encryption is enabled, then this field will be marked with a "Yes." You enter Encryption by clicking the Add Devices button, and then clicking Options
- **Last Update** -- Shows when device information was last updated
- **User Notes** -- User comments. You add notes by clicking Add Devices and entering text into the dialog box

Buttons

Edit Device -- Opens a dialog box for editing the device settings in the Device List.

Add New Device -- Opens a dialog box for adding new devices to the list. (You can also enter devices by performing an Inquiry.) This dialog box lets you enter information that will appear in the device list: device names, addresses, aliases, and comments.

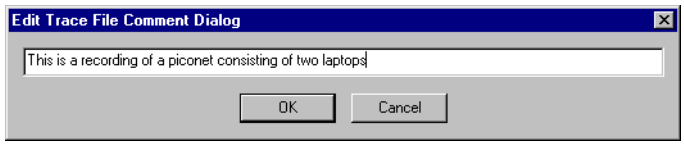
Remove Device -- Removes the selected device from the Device List.

10.3 Edit Comment

You can create, view, or edit the 100-character comment field associated with each Trace file.

Step 1 Select **Edit Comment** under **File** on the Menu Bar.

You see the **Edit comment for trace file** window:



Step 2 Create, view, or edit the comment.

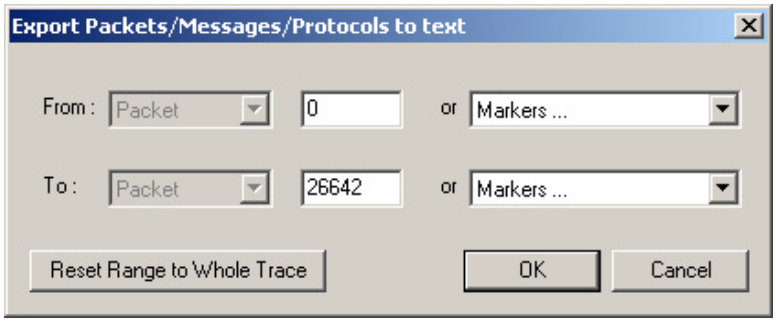
Step 3 Click **OK**.

10.4 Exporting Data

The Export command under the File menu allows you to export trace data for use in a spreadsheet, text editor or other utility. The Export command supports three formats:

Export »Packets toText (Packet View Format)

Saves all or part of a trace to a text file. Selecting this option opens a dialog box that prompts you for a range. Enter the range, then click **OK**. The data is then exported to a text file.

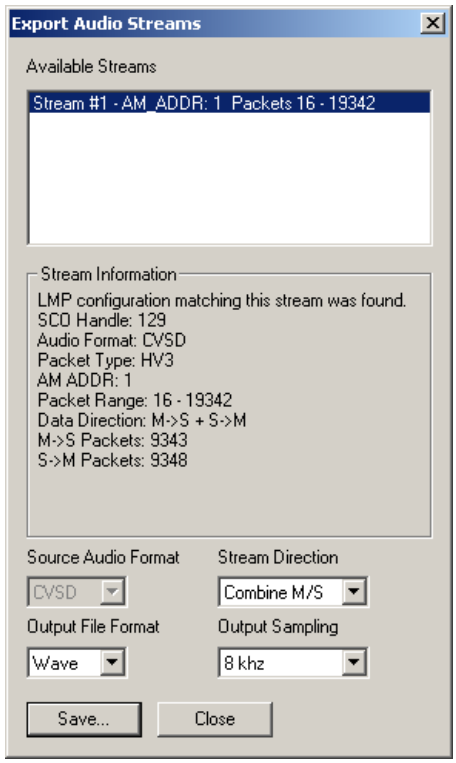


Export »Packets to CSV Text

Saves all or part of a trace to a Comma Separated Values (CSV) file suitable for viewing in a spreadsheet application. The steps are the same as those described above.

Export>>Audio Streams

Saves audio data into a file. Opens a dialog box with options for setting the Audio Source format, Output File format, Stream Direction, and Output Sampling.



10.5 File Information

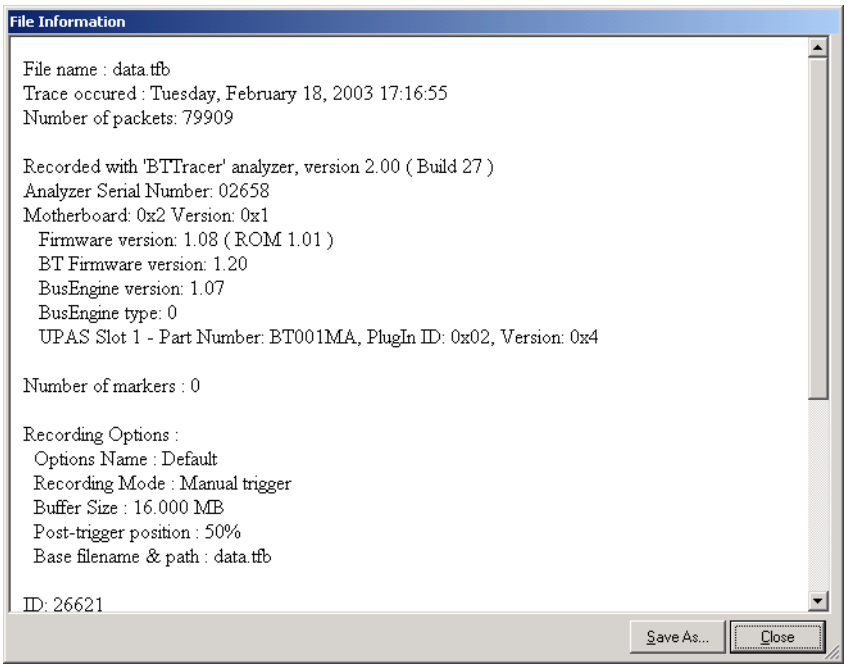
To display a File Information report,

- Select **File Information** under **Report** in the Menu Bar

  OR

  Click in the Tool Bar.

  You see the File Information screen:


File Information
File name : data.tfb
Trace occured : Tuesday, February 18, 2003 17:16:55
Number of packets: 79909
Recorded with 'BTTracer' analyzer, version 2.00 (Build 27)
Analyzer Serial Number: 02658
Motherboard: 0x2 Version: 0x1
Firmware version: 1.08 (ROM 1.01)
BT Firmware version: 1.20
BusEngine version: 1.07
BusEngine type: 0
UPAS Slot 1 - Part Number: BT001MA, PlugIn ID: 0x02, Version: 0x4
Number of markers : 0
Recording Options :
Options Name : Default
Recording Mode : Manual trigger
Buffer Size : 16.000 MB
Post-trigger position : 50%
Base filename & path : data.tfb
ID: 26621
Save As...
Close

The File Information report provides valuable information about how the recording was made, what the buffer settings were, what the trigger options were, and what version of all the analyzer hardware was used to make the recording.

10.6 Error Summary

The Error Summary command opens the **Traffic Summary** dialog box and displays an error summary of the current trace file. The dialog box allows you to go to a specific packet, and save the error file to a uniquely named file. See the discussion below on **Traffic Summary** for more information.

10.7 Timing Calculations

Starts the modeless calculator dialog for calculating various timing and bandwidth parameters in the recording file.

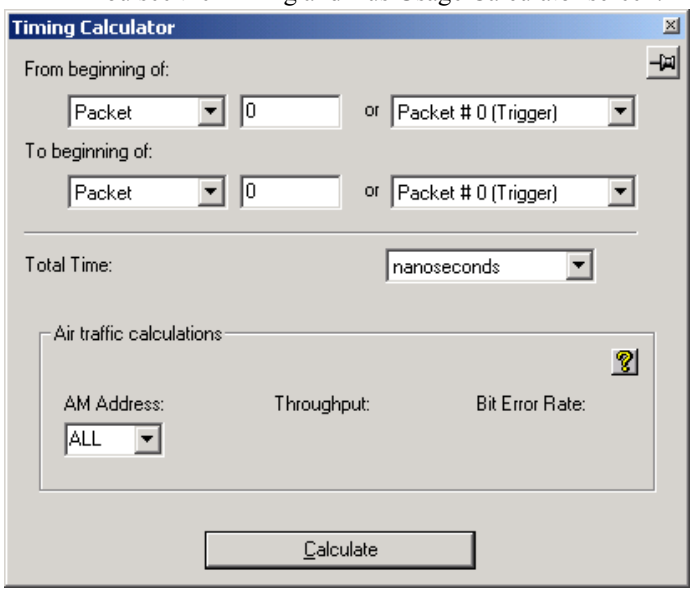
To display a File Information report,

- Select **Timing Calculations** under **Report** in the Menu Bar

  OR

  Click in the Tool Bar.

You see the Timing and Bus Usage Calculator screen:



To calculate bus usage and bit rate errors,

Step 1 Enter the range of packets to be examined in the text boxes marked "From packet" and "To packet."

Step 2 If you wish to limit your calculations to a single device, select the device's address from the AM Address drop-down menu.

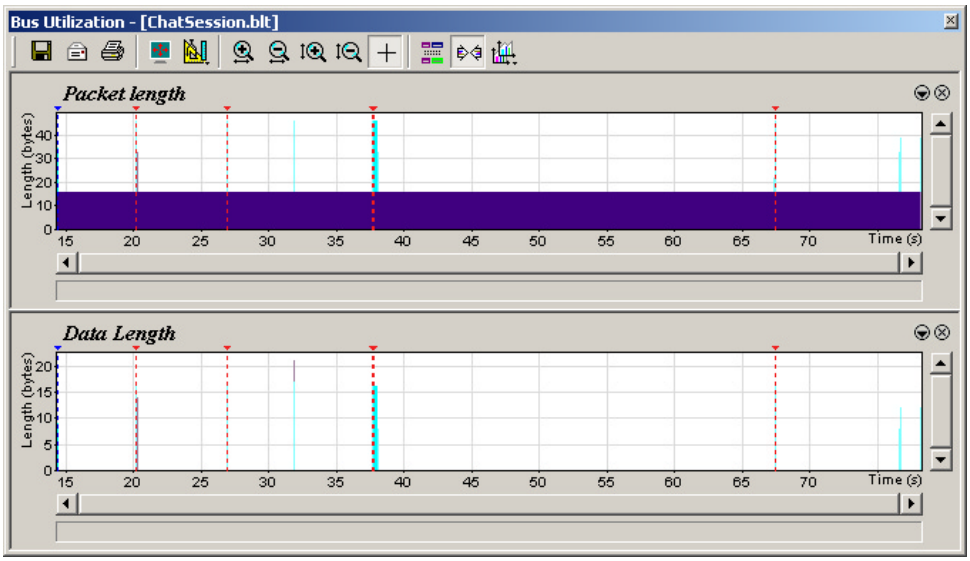
Step 3 Click the "Calculate" button.

At this point, bus usage will be calculated.

10.8 Bus Utilization

The **Bus Utilization** window displays a graph of bandwidth use within a displayed trace.

To open the Bus Utilization window, select **Report >Bus Utilization** or click the button marked . A window will open with graphs of Link Utilization, Data Throughput, and Packet Counts:



Bus Utilization Buttons

The Bus Utilization window has a row of buttons for changing the format of the displayed data and for exporting data:

The buttons have the following functions:

Save As - Saves the graphs as a bitmap file (*.bmp)

Email - Creates an email with a *.bmp file attachment of the graphs

Print

Full Screen

View Settings - opens a sub-menu with options for formatting the display. See "View Settings Menu" below.

Vertical zoom in

Vertical zoom out

Click and Drag zoom - Click diagonally to select and zoom in on part of the graph

Select Range

Sync and Graph areas - If two or more graphs are displayed, this button will synchronize the graphs to one another. Once synchronized, the positioning slider of one graph will move the other graphs

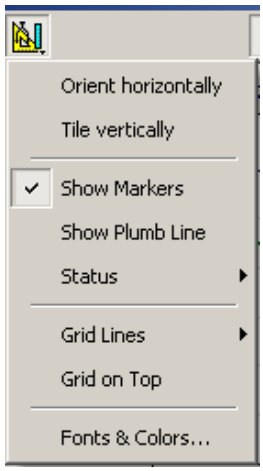
Horizontal zoom in

Horizontal zoom out

Graph Areas - Presents options for displaying additional graphs of data lengths, packet lengths, and percentage of bus utilized.

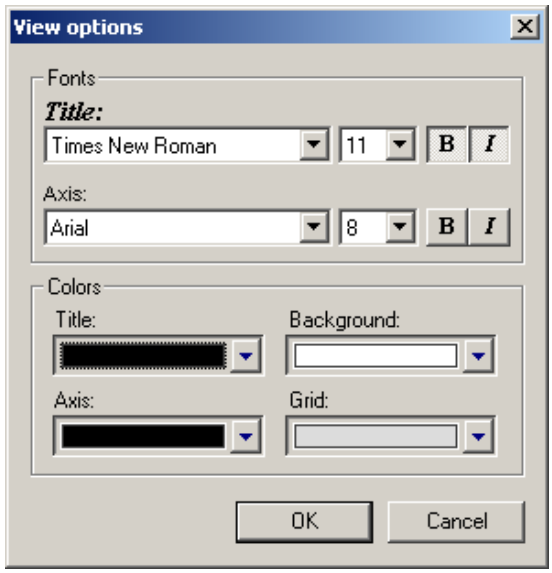
View Settings Menu

Clicking the View settings button causes a menu to open with options for formatting the display.



- **Orient Horizontally** - changes the orientation of bus usage to horizontal. After selecting this option, the menu will say "Orient Vertically."
- **Tile Vertically** - tiles the two graphs vertically (i.e., side by side).
- **Show Markers** - Places "tick" marks along the x axis of each graph.
- **Show Plumb Line** - Displays a vertical line that connects your cursor to the horizontal axis. As the mouse is moved, the status bar will show the packet and time frame to which the cursor is pointing.
- **Status** - Opens a sub-menu with the following options:
  - Bar - Displays a status bar at bottom of graph.
  - Tooltip - Causes a tooltip to appear if you position your mouse pointer over part of the graph and leave it there for a couple of seconds.
  - None - Turns off tooltips and the status bar.
- **Grid Lines** - Opens a sub-menu with the following options:
  - Both - Displays both X and Y axis gridlines.
  - X Axis - Displays X axis gridlines.
  - Y Axis - Display Y axis gridlines.
  - None - Turns off gridlines.
- **Grid on Top** - Moves the grid lines above the graph.

- **Fonts and Colors** - Opens a dialog box for setting the colors and fonts used in the graphs:

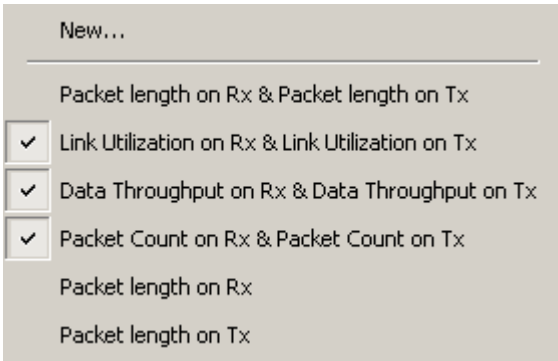


Graph Areas Menu

The Graph Areas menu allows you to view different information in the Bus Utilization window.

Step 1 Click the button.

The Graph Areas menu opens.


New...
Packet length on Rx & Packet length on Tx
Link Utilization on Rx & Link Utilization on Tx
Data Throughput on Rx & Data Throughput on Tx
Packet Count on Rx & Packet Count on Tx
Packet length on Rx
Packet length on Tx

Step 2 Select the data you want to appear in the Graph Areas window.

To change the properties in the Bus Utilizations graph, follow these steps:

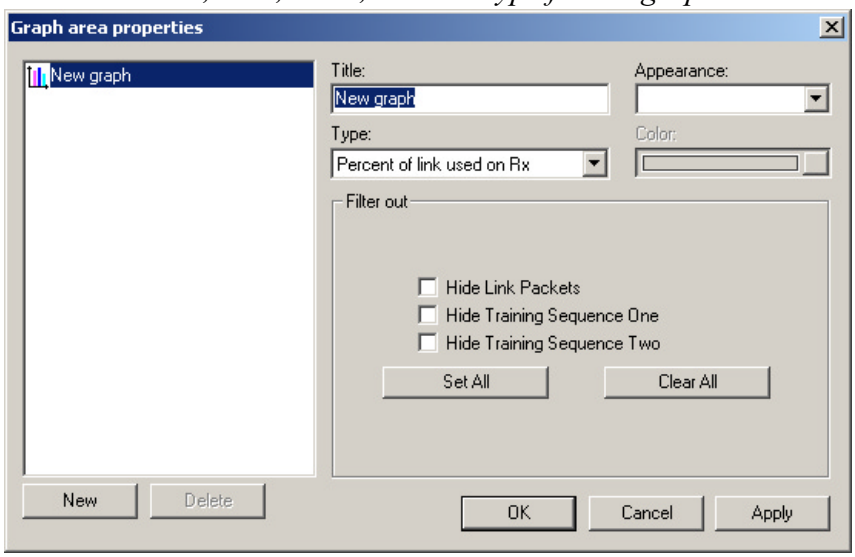
Step 1 In the **Graph Area**s menu, select the type of data to be displayed.

Step 2 Click **OK**.

Or

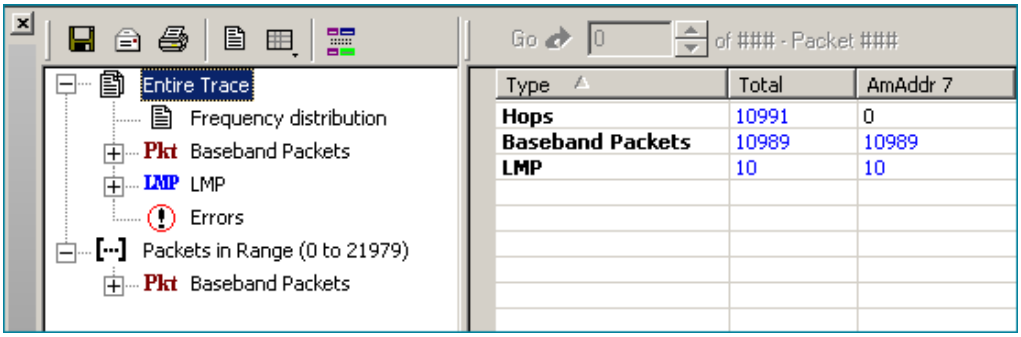
To make a new graph, click **New**.

The following dialog box will open. It will display options for setting the title, data, color, and line type for the graph.



10.9 Traffic Summary

The Traffic Summary dialog box displays a text summary of traffic captured in the current trace.



To open the Traffic Summary window, press .

The left pane displays a tree of the different protocol levels. Click the plus symbol (+) to expand the tree. The example above is fully expanded. The right pane displays a summary of the traffic for the selected level.

10.10 Encryption

Bluetooth encryption is a multi-staged process that provides devices with secure, encrypted communications. The pairing process begins with a device prompting the user for a Personal Identification Number (PIN).

When the right PIN is entered, the Slave begins an encryption setup dialogue with the Master. At the beginning of this dialogue, the Slave and the Master agree on a *Link Key*. A Link Key is a 128-bit value that the two devices use for authentication. When the Slave and Master agree on a Link Key, the Slave then negotiates for the transfer of the *Encryption Key* from the Master device. The Encryption Key is used to encrypt and decrypt messages. Once the Encryption Key is transferred, both devices use it to encrypt all subsequent communications.

In order for Merlin Mobile to decode encrypted traffic, it needs the *Link Key* for each Master-Slave connection for which encryption will be used. If you know the Link Key, you can enter the Key into the Encryption Options dialog box. If you do not know it, you give Merlin Mobile the PIN for a device and allow Merlin Mobile to discover the Link Key on its own. Once Merlin Mobile has the Link Key, it can capture the rest of what it needs by listening to the Master and Slave devices as they negotiate for the Encryption Key.

Configuring Merlin Mobile for Encryption

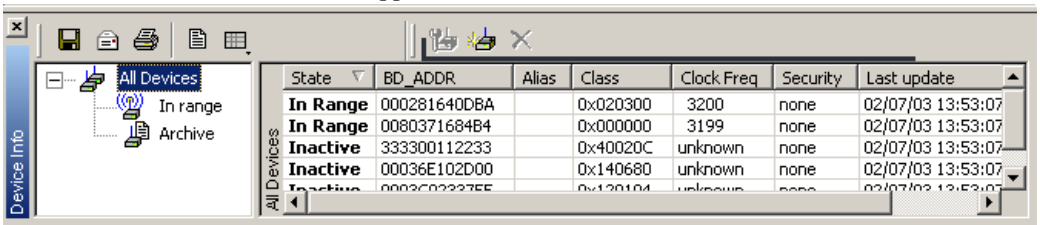
For Merlin Mobile to successfully decrypt traffic, two steps need to be performed: 1) Merlin Mobile needs to be given the PIN or Link Key for each Master-Slave connection; and 2) Recording needs to be begun *before* the Slave connects to the Master. If recording is begun prior to the creating the Master-Slave connection, Merlin Mobile will be able to obtain the encryption key and decode encrypted traffic.

The following steps show how to configure Merlin Mobile for encrypted traffic.

Note Be sure to begin the following process *prior* to connecting your Slave device to the Master or Merlin Mobile will not be able to capture the Link Key.

Step 1 Select **View >Device List**

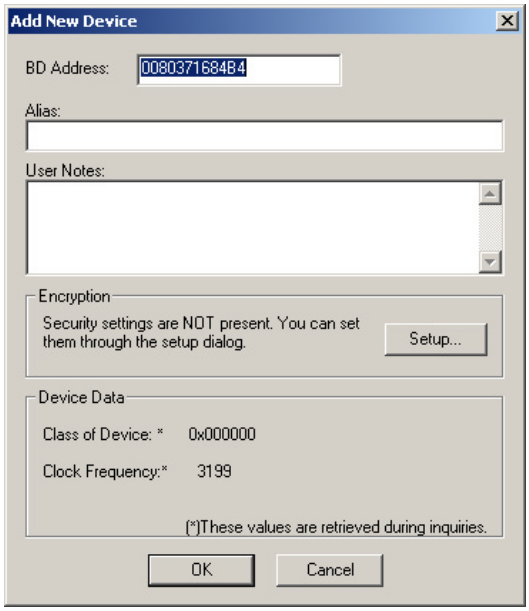
The Device List appears.



Step 2 Click in the row for the device of interest.

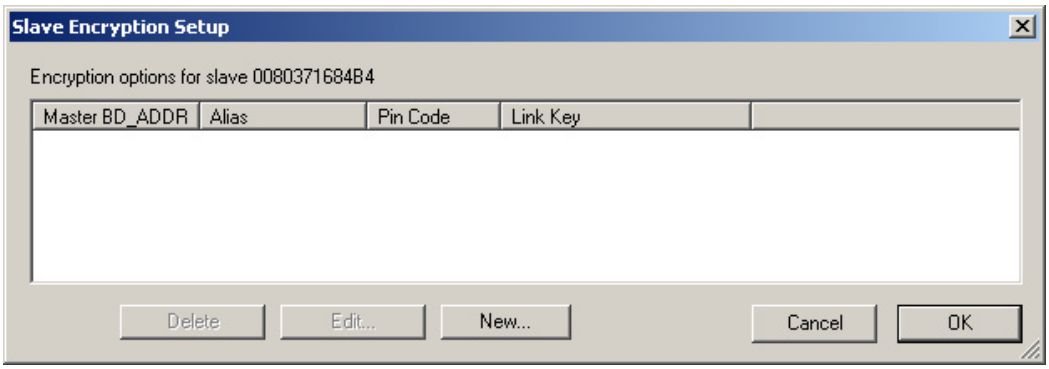
Step 3 Click the Edit Devices button

The following dialog box opens.



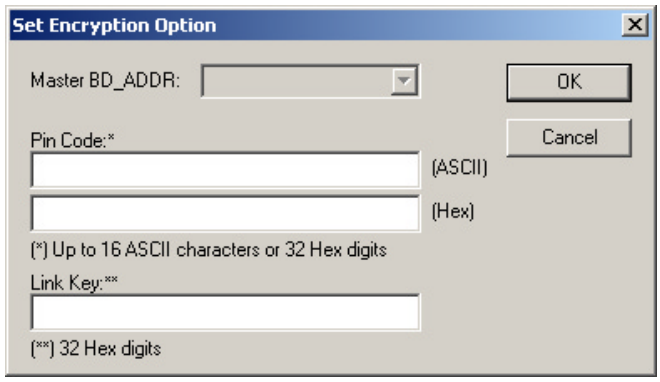
Step 4 Click the **Setup ...** button.

The following dialog box opens:



Step 5 Click the button marked **New**.

The following dialog box appears.



Step 6 Enter the appropriate Personal Identification Number (PIN) for the selected device to the box marked **PIN Code**. This PIN allows Merlin Mobile to learn the Link Key. If you do not have the PIN, skip to Step 5.

Note The PIN you provide should be the same used by the Slave. For example, if your Slave device requires a PIN of "1234", then enter the same PIN in the dialog box shown above.

Step 7 If you do not have the PIN, or if the Master and Slave have already agreed upon the Link Key, manually enter a Link Key as a 128 bit (sixteen byte) hex value into the box marked **Current Link Key**. If you have the PIN, you can skip this step.

Note If the Master and Slave were previously connected, they may already agree on the Link Key. In this case, you will need to provide Merlin Mobile with the Link Key and not simply the PIN.

Step 8 Click **OK**

The changes you have made are applied and the information is displayed in the **Slave Encryption Setup** dialog box as shown previously.

Step 9 Click **OK**.

The **Slave Encryption Setup** dialog box closes. Within the Device List, you should see a "Yes" in the Security field for the selected device.

How to Contact CATC

Type of Service	Contact
Call for technical support…	US and Canada: 1 (800) 909-2282 Worldwide: 1 (408) 727-6600
Fax your questions…	Worldwide: 1 (408) 727-6622
Write a letter…	Computer Access Technology Corp. Customer Support 2403 Walsh Avenue Santa Clara, CA 95051-1302
Send e-mail…	support@CATC.com
Visit CATC's web site…	http://www.CATC.com/

Warranty and License

Computer Access Technology Corporation (hereafter CATC) warrants this product to be free from defects in material, content, and workmanship, and agrees to repair or replace any part of the enclosed unit that proves defective under these terms and conditions. Parts and labor are warranted for one year from the date of first purchase.

The CATC software is licensed for use on a single personal computer. The software may be copied for backup purposes only.

This warranty covers all defects in material or workmanship. It does not cover accidents, misuse, neglect, unauthorized product modification, or acts of nature. Except as expressly provided above, CATC makes no warranties or conditions, express, implied, or statutory, including without limitation the implied warranties of merchantability and fitness for a particular purpose.

CATC shall not be liable for damage to other property caused by any defects in this product, damages based upon inconvenience, loss of use of the product, loss of time or data, commercial loss, or any other damages, whether special, incidental, consequential, or otherwise, whether under theory of contract, tort (including negligence), indemnity, product liability, or otherwise. In no event shall CATC's liability exceed the total amount paid to CATC for this product.

CATC reserves the right to revise these specifications without notice or penalty.

INDEX

Symbols

Numerics
1100 packet 90
1101 packet 90
A
Abort upload 40
Acknowledge 142
Action buttons 36, 97
Actions tab 96
Addr 116
Addresses
    AM_ADDR 91
    Bluetooth 60
    slave device 50
    target 61
AM Address 142
Analyzer
    describing Bluetooth 2
    set up 9
    status 40
API 4
Application installation 11
Architecture of Piconet 3
Arqn 116
ARQN condition 91
AT 124
Authentication 159
Automation Feature 4
AUX1 packet 90
B
Basic installation 9
Bit pattern, searching 145
Blue dot menus 100
Bluetooth
    BusEngine 6
    described 1
    device address 60
    first recording 18
    limited search 83
    recording traffic 105
    search for device 56

searching for devices 46
target address 61
BNEP 124
Bubble help 41
Buffer size 18, 74
Bus utilization 152
BusEngine
Bluetooth 6
Buttons
bus utilization 153
graph area 155
toolbar 36
C
CAC 116
Calculations, timing 151
CATC Technical Support 163
Certification 7
Channel connections, L2CAP 127
Clicked fields, menus in 121
Clock rate, match 81
Collapse data 118
Comments, editing 150
Components, physical 5
Configuring encryption 159
Connecting events 98
Connectors
data 7
physical 7
Correlation Value 82
Counters
connecting events 98
value 100
CRC 116
CRC error 94
D
Data
decoding 124
expand, collapse 118
filename 18
length 93
pattern 88, 93
searching by length 138
searching by pattern 145

transfer message 126
Debug file 19, 83
Decoding 124
Dedicated inquiry 19
Description of Merlin 2
Device
Bluetooth address 60
general search 48
search 46
search for Bluetooth 56
slave address 50
DH1, 2, 3 packet 90
Displaying information 115, 150
DM1 116
DM1, 2, 3 packet 90
Duration of search 56
DUT Recv/Xmit Freq 77
DV packet 90
E
Editing comments 150
Enable
debug file 83
Encryption 159
Environmental Conditions 7
Error summary 151
Errors
CRC 94
FEC 94
header length 95
HEC 94
invalid packet 94
payload length 95
Searching for 140
setting conditions for 94
sync loss 95
threshold exceeded 94
types of 88
Established Piconets 79
Events
conditions 91
connecting 98
sequencing 103
tab 88

trigger 18, 74
Exclusion search 146
Existing Piconet, recording 54
Expand data 118
Explicit NACK 142
External
input signals 88, 95
trigger form 102
F
Features 5
FEC Error 94
FHS packet 90
File information, displaying 150
File menu 33
Filename and data 18
Filter In/Out button 97
Filter Out/In 100
Filtering 89, 90
Find feature, using 146
Finding 140
Finding devices 46
Flow 116
Fonts 155
Force resynchronization 81
Frequencies, DUT 77
Frequency hops, hiding 120
G
General description 2
General features 5
General inquiry 19, 80, 83
General options
recording 71
General purpose output 102
Go to
DataLength 138
error 140
Header AM_Addr 138
L2Cap CID 140
Lmp Opcode 139
marker 136
packet types 137
packet/Message/Protocol 135
Graphs

areas menu 155
bus utilization 153
buttons 155
Grid
lines 154
on Top 154
Groups, events 88
H
HDLC 124
Headers
AM_Addr 138
length error 95
packets 90
payload 91
HEC 116
HEC Error 94
Help menu 35
Hexadecimal patterns, searching 145
HID 124
Hiding 120, 121
Higher protocols, decoding 123
High-pulse output 102
Hops
hiding 120
reduced mode 64
sequence 19
Hot keys 41
Humidity 7
HV1, 2, 3 packet 90
I
Idle 116
Implicit NACK 142
Information, interpreting 115
Input signals 88, 95
Inquiry
dedicated 19
general 83
perform/skip 45
recording 19
timeout 19, 82
Installation
basic 9
Interpreting a trace 115

Intersection search 146
Introduction 1
Invalid packet type error 94
K
Keyboard shortcuts 41
L
L_CH (Logical Channel) 92, 116
L2CAP
    channel connections 127
    CID, searching 140
    described 124
    messages 121, 123, 126
L2FL 116
Len 116
Length of data 93
License 163
Limited inquiry 19
Linking events 98
LMP
    described 124
    messages 123, 126
    Opcode 139
Logical Channel 92
Long pattern, searching 145
Loss of sync
    searching for 140
    timeout 82
Low-pulse output 102
M
Manual trigger 7, 18, 74
Markers
    editing and clearing 117
    searching 136
    setting 116
Master
    and slave 142
    switch 81
Master/address 60
Match clock rate 81
Memory, Recording 7
Menus
    blue dots in events 100
    clicked fields 121

pulldown 33
view settings 154
Merlin
configure encryption 159
description of 2
Message
searching 135
Messages
LMP, L2CAP 123, 126
transfer 126
Modes
test, recording in 64
N
NULL packet 90
Nulls, hiding 120
O
OBEX 124
Opcode 116
Operating temperature 7
Options
general recording 71
name 18
search 62
Orient horizontally 154
Output signals, enabling 102
Overview 1, 33
P
Package dimensions 7
Packets
1100, 1101 90
AUX1 90
DM1, 2, 3 90
DV 90
FHS 90
headers 88, 90
headers in 90
hiding 112
HV1, 2, 3 90
invalid type error 94
NULL 90
POLL 90
searching 135, 137
types 90, 142

viewing 126
Page
sync and record 88
Paging traffic 82
Passive sync and record 78
Patterns, data 93
Payload
headers 88, 91
length error 95
Percentage of triggering 75
Phone numbers, Technical Support 163
Physical Components 5
Piconet
established devices 79
master address 60
private device 79
recording 19, 50, 54
recording traffic on 44
sample 3
search options 62
slave address 50
sync and record 79
synchronizing 50
target address 61
Wizard 51
PIN 159
Pkt 124
Polls
hiding 120
POLL packet 90
Position of trigger 75
Post triggering, percentage 75
Power
LED 7
Switch 7
PPP 124
Pre-triggering 75
Private Device Piconets 79
Program
installation 11
Progress indicator, recording 38
Protocol
Analyzer 2

Architecture 3
decoding 124
searching 135
Pull-down menus 33
Pulse low signal 102
Pulse toggle signal 102
R
Reading a trace 115
Record inquiry 83
Record menu 33
Recording
Bluetooth traffic 18, 105
existing Piconet 54
LED 7
memory 7
mode 19
Piconet 50
progress indicator 38
reduced hop mode 64
session 21
type 73
Recording Options
events 88
general 18, 71, 73
in Wizard 51
saving 104
Recording type 54
Recv, DUT freq 77
Reduced hops 64
Reports
menu 33
Restart button 98
Resynchronization, forced 81
RFCOMM 124
S
Sample
Piconet 3
recording 21
Saving
recording options 104
SDP Msg 124
Search 48
duration of 56

general 58
Search menu 33
Search options 62
Search type 46, 56
Searching
by data pattern 145
complex 140
data length 138
for bit pattern 145
for bit patterns 145
for errors 140
Header AM_Addr 138
L2Cap CID 140
Lmp Opcode 139
packet types 137
recorded traffic 135
Security 159
SEQN condition 91
Sequence
event 103
Set marker 116
Setup
menu 33
Shortcuts, keyboard 41
Show markers 154
Show plumb Line 154
Signalling
message 126
Signals
input 88, 95
outputs, enabling 102
Size of buffer 74
Slave device, address 50
Slave switch 81
Snapshot 18, 74
Soft Bit Error, searching 140
Software
installation 11
overview 33
Special Interest Groups (SIGs) 1
Specifications 7
Status
status bar 154

Status bar 38
Status of Analyzer 40
Storage temperature 7
Summary
    error 151
    traffic 156
Support, technical 163
Switches 7, 81
Sync
    and record 78
    loss error 95
    loss of, searching 140
    timeout, loss of 82
    window 82
Synchronization, forced 81
Synchronize Piconet 50
Synchronized LED 7
T
Tabs
    recording events 88
    recording, general 18, 72
    recording, modes 19
    recording, options 71
Technical Support 163
Temperature tolerances 7
Test debug 83
Test mode, recording in 64
Threshold Exceeded error 94
TID 116
Tile vertically 154
Time Stamp 116
Timeout
    inquiry 82
    loss of sync 82
Timeslot filtering 89
Timing calculations 151
Tips, tool 41
Toggle signal 102
Toolbar 36
Tooltips 41, 116, 126
Trace
    filename 18
    reading 115

sample 21
Traffic
Bluetooth 105
generation 6
hiding 121
on Piconet 54
paging 82
recording 62
recording on piconet 44
searching 135
summary 156
Trail 116
Transfer message, data 126
Trigger
event 74
external form 102
LED 7
position 18, 75
post triggering 75
recording, manual 74
Type of recording 73
U
Unassociated traffic, hide 121
Union search 146
V
Values, changing counters 100
View
menu 33
options 36
packets 126
settings menu 154
W
Warranty 163
Weight 7
Window menu 35
Wizard
Piconet 51
X
Xmit, IUT freq 77
Z
Zoom 41